Cited Document 2

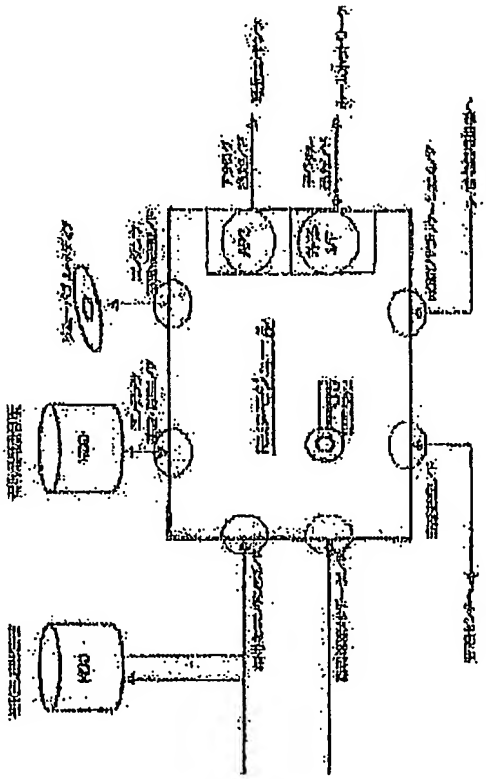
DEVICE AND METHOD FOR RECEIVING CONTENTS, STORAGE MEDIUM AND SERVER

Publication number: JP2002123496 (A)
Publication date: 2002-04-26
Inventor(s): EZAKI TADASHI +
Applicant(s): SONY CORP +
Classification:
- International: *G06F13/00; G06F21/00; G06Q30/00; G10K15/02; H04L9/08; H04N5/44; H04N7/16; H04N7/167;* G06F13/00; G06F21/00; G06Q30/00; G10K15/02; H04L9/08; H04N5/44; H04N7/16; H04N7/167; (IPC1-7): G06F13/00; G06F15/00; H04L9/08; H04N5/44; H04N7/16; H04N7/167
- European: G06F21/00N7D; G06Q30/00C
Application number: JP20000316395 20001017
Priority number(s): JP20000316395 20001017

Also published as:
US2002120574 (A1)
US7035827 (B2)

Abstract of JP 2002123496 (A)

PROBLEM TO BE SOLVED: To provide a contents receiver corresponding to a plurality of RMPs(Right Management and; Protection) systems drawn up in each contents distribution system. SOLUTION: Only formats for regulating the specifications of the RMPs composed of information such as contents charging, security and copyright protection are unified. Each contents provider inputs enciphered contents and right processing information in a format conforming to the unified specification. A contents user side can decode and utilize contents, regardless of their PMP systems, on the same contents receiver only by preparing a plurality of functions corresponding to the respective RMP systems.



Cited Document 2

(19)日本国特許庁（JP）　(12)公開特許公報(A)　(11)特許出願公開番号
特開2002－123496
(P2002－123496A)
(43)公開日　平成14年4月26日(2002.4.26)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
G06F	15/00	330	G06F	15/00	330Z 5B085
	13/00	540		13/00	540S 5C026
H04L	9/08		H04N	5/44	Z 5C064
H04N	5/44			7/16	C 5J104
	7/16		H04L	9/00	601A

審査請求　未請求　請求項の数29　OL　(全 29 頁)　最終頁に続く

(21)出願番号　特願2000－316395(P2000－316395)

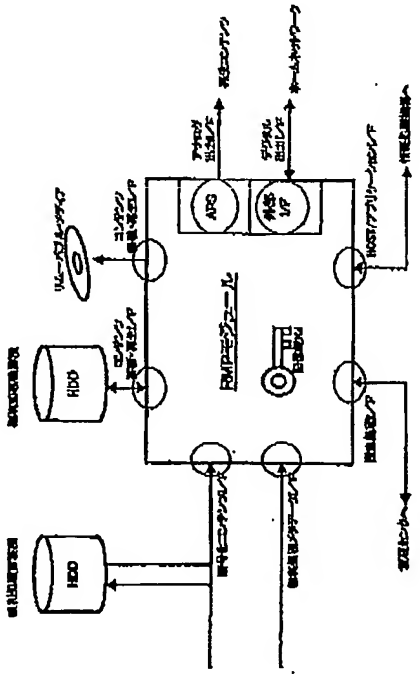
(22)出願日　平成12年10月17日(2000.10.17)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　江▲崎▼　正
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　(外２名)

最終頁に続く

(54)【発明の名称】　コンテンツ受信装置及びコンテンツ受信方法、記憶媒体、並びにサーバ

(57)【要約】
【課題】　各コンテンツ配信システム毎に策定される複数のＲＭＰ (Right Management & Protection) 方式に対応するコンテンツ受信機を提供する。
【解決手段】　コンテンツ課金・セキュリティ・著作権保護などの情報からなるＲＭＰの仕様を規定する書式のみを統一化する。各コンテンツ提供事業者は統一仕様に則った形式で暗号化コンテンツや権利処理情報をコンテンツに入力する。コンテンツ利用者側では、各々のＲＭＰ方式に対応した機能を複数用意しておくだけで、どのようなＲＭＰ方式に基づくコンテンツであっても、同じコンテンツ受信機上で復号化して利用に供することができる。



1

【特許請求の範囲】

【請求項1】所定の権利管理・保護（Right Management & Protection：RMP）方式に則って配信されるコンテンツを受信するコンテンツ受信装置であって、

配信コンテンツを受信するコンテンツ受信手段と、

受信コンテンツの権利管理・保護方式を識別する識別手段と、

前記識別手段による識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理手段と、を具備することを特徴とするコンテンツ受信装置。

【請求項2】権利管理・保護方式は、コンテンツの暗号化方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、ＡＰＳ（Analog Protection System：マクロビジョンやＣＧＭＳ（Copy Generation Management System）など）、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目を規定することを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項3】複数種類の権利管理・保護モジュールを備え、

前記権利処理手段は、前記識別手段による識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行う、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項4】権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得手段を備え、

前記権利処理手段は、前記識別手段による識別結果に基づいて前記権利管理・保護モジュール取得手段を介して外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項5】権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成手段を備え、

前記権利処理手段は、前記権利管理・保護モジュール生成手段によって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項6】コンテンツを蓄積するコンテンツ蓄積手段を含むことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項7】コンテンツを蓄積するコンテンツ蓄積手段を含み、

前記権利処理手段による権利処理前のコンテンツを前記コンテンツ蓄積手段に格納する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項8】コンテンツを蓄積するコンテンツ蓄積手段を含み、

前記権利処理手段による権利処理後のコンテンツを前記

2

コンテンツ蓄積手段に格納する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項9】前記コンテンツ受信手段は所定の鍵で暗号化された形式で配信されるコンテンツを受信し、

コンテンツを蓄積するコンテンツ蓄積手段をさらに含み、

前記権利処理手段は、受信した暗号化コンテンツを復号化し、他の鍵で再暗号化した後にコンテンツ蓄積手段に格納する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項10】前記コンテンツ受信手段は、所定の鍵で暗号化された形式で配信されるコンテンツ、並びに該鍵を暗号化した暗号化鍵を受信し、

コンテンツを蓄積するコンテンツ蓄積手段をさらに含み、

前記権利処理手段は、受信した暗号化鍵を復号化し、他の鍵で再暗号化した後に暗号化コンテンツとともにコンテンツ蓄積手段に格納する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項11】前記権利処理手段は、受信コンテンツの権利処理のログを蓄積することを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項12】前記権利処理手段は、権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってＡＰＳ（Analog Protection System）処理して外部出力する、ことを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項13】前記権利処理手段は、権利処理後のコンテンツを暗号化して外部出力することを特徴とする請求項1に記載のコンテンツ受信装置。

【請求項14】所定の権利管理・保護（Right Management & Protection：RMP）方式に則って配信されるコンテンツを受信するコンテンツ受信方法であって、

配信コンテンツを受信するコンテンツ受信ステップと、

受信コンテンツの権利管理・保護方式を識別する識別ステップと、

前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とするコンテンツ受信方法。

【請求項15】権利管理・保護方式は、コンテンツの暗号化方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、ＡＰＳ（Analog Protection System：マクロビジョンやＣＧＭＳ（Copy Generation Management System）など）、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目を規定することを特徴とする請求項14に記載のコンテンツ受信方法。

【請求項16】複数種類の権利管理・保護モジュールを備え、

前記権利処理ステップでは、前記識別ステップによる識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行う、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項１７】前記識別ステップによる識別結果に基づいて、該当する権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得ステップをさらに備え、

前記権利処理ステップでは、前記権利管理・保護モジュール取得ステップにより外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項１８】権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成ステップをさらに備え、

前記権利処理ステップでは、前記権利管理・保護モジュール生成ステップによって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行う、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項１９】受信したコンテンツを蓄積するコンテンツ蓄積ステップを含むことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２０】前記権利処理ステップによる権利処理前のコンテンツを格納するコンテンツ蓄積ステップを含むことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２１】前記権利処理ステップによる権利処理後のコンテンツを格納するコンテンツ蓄積ステップを含むことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２２】前記コンテンツ受信ステップでは所定の鍵で暗号化された形式で配信されるコンテンツを受信し、

前記権利処理ステップにおいて復号化した受信コンテンツを他の鍵で再暗号化した後に格納するコンテンツ蓄積ステップを備える、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２３】前記コンテンツ受信ステップでは、所定の鍵で暗号化された形式で配信されるコンテンツ、並びに該鍵を暗号化した暗号化鍵を受信し、

前記権利処理ステップにおいて復号化した鍵を他の鍵で再暗号化した後に暗号化コンテンツとともに格納するコンテンツ蓄積ステップを備える、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２４】前記権利処理ステップにおける受信コンテンツの権利処理のログを蓄積するログ蓄積ステップを備えることを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２５】前記権利処理ステップによる権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってＡＰＳ（Analog Protection System）処理して外部出力する外部出力ステップを備える、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２６】前記権利処理ステップによる権利処理後のコンテンツを暗号化して外部出力する外部出力ステップを備える、ことを特徴とする請求項１４に記載のコンテンツ受信方法。

【請求項２７】所定の権利管理・保護（Right Management & Protection：ＲＭＰ）方式に則って配信されるコンテンツの受信処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、

配信コンテンツを受信するコンテンツ受信ステップと、

受信コンテンツの権利管理・保護方式を識別する識別ステップと、

前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とする記憶媒体。

【請求項２８】それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、

権利管理・保護方式の識別情報を含んだ要求に応答して、該当する権利管理・保護モジュールを送信する手段と、を備えることを特徴とするサーバ。

【請求項２９】それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、

識別情報に基づく問合せに応答して、該当する権利管理・保護モジュールを用いてコンテンツを変換する手段と、を具備することを特徴とするサーバ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、放送波やネットワークなどを介して配信されるコンテンツを受信するコンテンツ受信装置及びコンテンツ受信方法に係り、特に、映画や音楽などの暗号化された形式で配信される有料コンテンツを特定の利用者が受信するコンテンツ受信装置及びコンテンツ受信方法に関する。

【０００２】更に詳しくは、本発明は、映画や音楽などのコンテンツ制作・提供業者が放送事業者やインターネット・サービス・プロバイダなどの仲介業者を介して配信する暗号化コンテンツを受信するコンテンツ受信装置及びコンテンツ受信方法に係り、特に、コンテンツ制作・提供業者自身がコンテンツ利用に関する課金やセキュリティなどを制御可能な形態で配信するコンテンツを受信するコンテンツ受信装置及びコンテンツ受信方法に関する。

5

【0003】

【従来の技術】昨今の情報技術の革新に伴い、映像や音楽など、さまざまなメディアがデジタル化されたコンテンツとしてコンピュータなどの情報機器上で取り扱われるようになってきている。さらに、情報通信技術の発達により、これらコンテンツを、衛星や地上波などの放送、あるいはインターネットのような広域的なネットワークを利用して、配信することができる。

【0004】映像コンテンツや音楽コンテンツの配信は一部で既に実施されている。コンテンツ配信技術によれば、旧来の商品流通経路や物理的な媒体を省略することができる。また、遠隔地の消費者であっても、所望の映像・音楽ソフトを容易に入手することができる。また、コンテンツ制作・提供業者側の立場では、迅速且つ効率的なコンテンツ販売によってより高い利益をあげることにより、コンテンツ制作意欲が増し、業界全体の発展にもつながる

【0005】例えば、テレビ受信機が大容量のハード・ディスク装置を内蔵していることを前提としたサーバ型・蓄積型の放送システムにおいては、映画などのコンテンツを、放送局やその他のコンテンツ配信業者において暗号化して配信し、コンテンツ購入者すなわち視聴者に対して暗号解読用の鍵を配布時に課金することによって確実に利益を確保することができる。

【0006】このようなコンテンツ受信形式のことをCAS（Conditional Access Systen（限定受信））方式とも呼ぶ。図14には、CASベースのコンテンツ配信システムの概観構成を図解している。

【0007】同図に示すコンテンツ配信システムでは、映像や音楽などの配信用コンテンツを制作又は提供するコンテンツ・プロバイダと、コンテンツ・プロバイダが提供するコンテンツを、放送波やネットワークを経由して消費者に配信するコンテンツ配信事業者と、コンテンツを受信する消費者すなわち一般ユーザの3者で構成される。

【0008】コンテンツ配信事業者は、例えば、BS（Broadcasting Satellite：放送衛星）CS（Communication Satellite：通信衛星）など放送衛星を利用した放送事業者、地上波を利用した放送事業者、あるいは、インターネットへの接続サービス並びにインターネット上での各種情報コンテンツ提供サービスを運営するインターネット・サービス・プロバイダなどで構成される。

【0009】一般ユーザは、例えば自宅内に配信コンテンツを受信するコンテンツ受信機を設置している。放送波を介したコンテンツを受信するコンテンツ受信機は、例えばSTB（Set Top Box）のようなテレビ受信機でよい。また、インターネット経由でコンテンツを受信するコンテンツ受信機は、例えば、パーソナル・コンピュータ（PC）のような一般的な計算機システムでよい。コンテンツ受信機は、ハード・ディスク装置を内蔵し、

6

長時間すなわち大量の映像・音楽コンテンツを蓄積可能な蓄積型放送対応受信機であることが好ましい。

【0010】コンテンツ受信機が放送波を介してコンテンツを受信するためには、各放送事業者毎に対応したCAS（限定受信）カードを装備しておく必要がある。また、インターネット経由でコンテンツを受信するためには、所定のインターネット・サービス・プロバイダからあらかじめユーザ・アカウント（利用者資格）を取得するとともに、コンテンツ購入時に最寄のアクセス・ポイントを介してインターネット接続する必要がある。

【0011】放送事業者がコンテンツ配信に要する費用や利益を回収するためには、例えばCASカード（あるいはCASを内蔵した受信機）購入時を利用すればよい。また、インターネット・サービス・プロバイダがコンテンツ配信に要する費用や利益を回収するためには、例えば、月々支払われる会費にコンテンツ利用料相当額を上乗せすればよい。但し、CASシステムやユーザ・アカウントによる課金方式は、コンテンツ配信事業者が個々の消費者すなわちコンテンツ利用者に対する課金を制御することを目的とするものであり、コンテンツ・プロバイダの制御下にはない。言い換えれば、コンテンツ・プロバイダは、コンテンツ配信事業者車体のCASなどを利用しても、自らの利益を確保することはできない。

【0012】コンテンツ・プロバイダが一般消費者からコンテンツ利用料を徴収するためには、コンテンツ・プロバイダ自身がコンテンツ課金、セキュリティ、著作権保護などのコンテンツ提供方式（以下では、RMP（Right Management & Protection）と呼ぶ）を策定することが挙げられる。RMPの中には、より具体的には、暗号化の方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、APS（Analog Protection System：マクロビジョンやCGMS（Copy Generation Management System）など）、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目が含まれている。コンテンツの利用者・消費者側では、コンテンツ・プロバイダに対応するRMPモジュールを実装したコンテンツ受信機を用意することで、コンテンツ・プロバイダを供給源とする配信コンテンツを成功裏に購入し、利用すなわち視聴することができる。また、管理センタのようなコンテンツ・プロバイダ外の決済機関に対して課金情報の一括管理を委ねるようにしてもよい。

【0013】しかしながら、コンテンツ課金、セキュリティ、著作権保護に関するRMP方式は、一般に、各コンテンツ・プロバイダが提供するコンテンツ配信システム毎に区々に策定するのが現状である。複数の方式が混在する環境下では、同じ音楽コンテンツ配信、映画コンテンツ配信であっても、コンテンツ配信システムが相違すると同じコンテンツ受信機上では復号化できない、す

なわちコンテンツを利用できないという事態に陥る。

【0014】例えば、コンテンツ利用者が複数のコンテンツ・プロバイダすなわち配信システムからコンテンツを購入しようとすると、各配信システム毎にコンテンツ受信機のハードウェア又はソフトウェアを用意しなければならず、利用者に不便であったり、あるいは余計な出費が必要となる。また、コンテンツ購入方法が面倒であることの帰結として、利用者のコンテンツ買い控えが生じると、コンテンツ提供・配信事業の利益が伸び悩み、事業全体が沈静化してしまうことになりかねない。

【0015】

【発明が解決しようとする課題】本発明の目的は、映画や音楽などの暗号化された形式で配信される有料コンテンツを特定の利用者が好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【0016】本発明の更なる目的は、映画や音楽などのコンテンツ制作・提供業者が放送事業者やインターネット・サービス・プロバイダなどの仲介業者を介して配信する暗号化コンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【0017】本発明の更なる目的は、コンテンツ制作・提供業者自身がコンテンツ利用に関する課金やセキュリティなどを制御可能な形態で配信するコンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【0018】本発明の更なる目的は、各コンテンツ配信システム毎に策定される複数のRMP (Right Management & Protection) 方式に対応することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することにある。

【0019】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第1の側面は、所定の権利管理・保護 (Right Management & Protection; RMP) 方式に則って配信されるコンテンツを受信するコンテンツ受信装置であって、配信コンテンツを受信するコンテンツ受信手段と、受信コンテンツの権利管理・保護方式を識別する識別手段と、前記識別手段による識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理手段と、を具備することを特徴とするコンテンツ受信装置である。

【0020】コンテンツの制作・提供事業者は、RMPと呼ばれる権利管理・保護方式に従って暗号化などの保護された形式でコンテンツを配信する。一般に、コンテンツ制作・提供事業者毎に区々の権利管理・保護方式を採用する。

【0021】本発明の第1の側面に係るコンテンツ受信装置によれば、権利管理・保護方式の仕様を規定する書式のみを統一化するだけで、識別手段が受信コンテンツの権利管理・保護方式を識別して、権利処理手段は、該識別結果に基づいて該当する権利管理・保護方式を選択的に用いて受信コンテンツを権利処理することができる。

【0022】したがって、それぞれの権利管理・保護方式に対応した機能をあらかじめ用意しておくだけで、どの権利管理・保護方式に則ったコンテンツを受信した場合であっても、1台のコンテンツ受信機を用いて複数の異なるコンテンツ配信方式に対応することができる。すなわち同じコンテンツ受信機上でコンテンツを復号化して利用に供することができ、配信システム毎の受信機などの機器を用意する必要がなくなる。

【0023】また、各コンテンツ制作・提供・配信事業者間では、RMP仕様記述などのコンテンツ配信方式の規格化をめぐる争いを沈静化することができる。また、各コンテンツ制作・提供・配信事業者間における配信コンテンツの互換性や融通性を向上させることができる。また、コンテンツ利用者においては、利便性が高まる。

【0024】ここで言う権利管理・保護方式は、コンテンツの暗号化方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、APS (Analog Protection System：マクロビジョンやCGMS (Copy Generation Management System) など)、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目を規定するものである。

【0025】コンテンツ受信装置は、あらかじめ複数種類の権利管理・保護モジュールを備えておいてもよい。このような場合、前記権利処理手段は、前記識別手段による識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行うことができる。

【0026】あるいは、コンテンツ受信装置は、権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得手段を備えていてもよい。このような場合、前記権利処理手段は、前記識別手段による識別結果に基づいて前記権利管理・保護モジュール取得手段を介して外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【0027】あるいは、コンテンツ受信装置は、権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成手段を備えていてもよい。このような場合、前記権利処理手段は、前記権利管理・保護モジュール生成手段によって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことかできる。

【0028】また、コンテンツ受信装置は、コンテンツを蓄積するコンテンツ蓄積手段を含んでいてもよい。例

えば、前記権利処理手段による権利処理前、あるいは権利処理後のコンテンツを前記コンテンツ蓄積手段に格納することができる。

【0029】前記コンテンツ受信手段が受信するコンテンツは、例えば、所定の鍵で暗号化されている。このような場合、前記権利処理手段は、受信した暗号化コンテンツを復号化し、他の鍵で再暗号化した後にコンテンツ蓄積手段に格納するようにしてもよい。このような構成により、権利処理後のコンテンツをさらに保護することができる。

【0030】また、前記コンテンツ受信手段が受信するコンテンツは、例えば、所定の鍵で暗号化された形式で配信されているとともに、さらに該鍵を暗号化した暗号化鍵も受信する。このような場合、前記権利処理手段は、受信した暗号化鍵を復号化し、他の鍵で再暗号化した後に暗号化コンテンツとともにコンテンツ蓄積手段に格納するようにしてもよい。このような構成により、権利処理後のコンテンツをさらに保護することができる。

【0031】また、前記権利処理手段は、受信コンテンツの権利処理のログを蓄積するようにしてもよい。このような場合、例えば、蓄積されたログを所定の決済機関に定期的あるいは不定期的に送信することにより、決済機関では正確な課金処理を行うことができる。

【0032】また、前記権利処理手段は、権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってＡＰＳ（Analog Protection System）処理して外部出力するようにしてもよい。このような場合、権利処理後のビデオ再生信号などを保護することができる。

【0033】また、前記権利処理手段は、権利処理後のコンテンツを暗号化して外部出力するようにしてもよい。このような場合、例えばＩＥＥＥ　１３９４のようなホーム・ネットワーク経由で他の情報機器にコンテンツを転送する場合や、ＬＡＮ経由でパーソナル・コンピュータ（ＰＣ）のような計算機システムにコンテンツを送信してアプリケーションを用いて処理する場合であっても、コンテンツを保護することができる。

【0034】また、本発明の第２の側面は、所定の権利管理・保護（Right Management & Protection：ＲＭＰ）方式に則って配信されるコンテンツを受信するコンテンツ受信方法であって、配信コンテンツを受信するコンテンツ受信ステップと、受信コンテンツの権利管理・保護方式を識別する識別ステップと、前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とするコンテンツ受信方法である。

【0035】本発明の第２の側面に係るコンテンツ受信方法によれば、権利管理・保護方式の仕様を規定する書式のみを統一化するだけで、識別ステップが受信コンテンツの権利管理・保護方式を識別して、権利処理ステップでは、該識別結果に基づいて該当する権利管理・保護方式を選択的に用いて受信コンテンツを権利処理することができる。

【0036】前記権利処理ステップでは、前記識別ステップによる識別結果に基づいて、対応する権利管理・保護モジュールを選択して受信コンテンツの権利処理を行うようにしてもよい。

【0037】あるいは、前記識別ステップによる識別結果に基づいて、該当する権利管理・保護モジュールを外部から取得する権利管理・保護モジュール取得ステップをさらに備えていてもよい。このような場合、前記権利処理ステップでは、前記権利管理・保護モジュール取得ステップにより外部から取得された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【0038】あるいは、権利管理・保護方式の仕様記述に従い権利管理・保護モジュールを自動生成する権利管理・保護モジュール生成ステップをさらに備えていてもよい。このような場合、前記権利処理ステップでは、前記権利管理・保護モジュール生成ステップによって生成された権利管理・保護モジュールを用いて受信コンテンツの権利処理を行うことができる。

【0039】また、受信したコンテンツを蓄積するコンテンツ蓄積ステップを含んでいてもよい。例えば、前記権利処理ステップによる権利処理前、あるいは権利処理後のコンテンツを格納するようにしてもよい。

【0040】また、前記コンテンツ受信ステップでは所定の鍵で暗号化された形式で配信されるコンテンツを受信するような場合、前記権利処理ステップにおいて復号化した受信コンテンツを他の鍵で再暗号化した後に格納するコンテンツ蓄積ステップを備えていてもよい。

【0041】また、前記コンテンツ受信ステップでは、所定の鍵で暗号化された形式で配信されるコンテンツ、並びに該鍵を暗号化した暗号化鍵を受信するような場合、前記権利処理ステップにおいて復号化した鍵を他の鍵で再暗号化した後に暗号化コンテンツとともに格納するコンテンツ蓄積ステップを備えるようにしてもよい。

【0042】また、前記権利処理ステップにおける受信コンテンツの権利処理のログを蓄積するログ蓄積ステップを備えていてもよい。このような場合、例えば、蓄積されたログを所定の決済機関に定期的あるいは不定期的に送信することにより、決済機関では正確な課金処理を行うことができる。

【0043】また、前記権利処理ステップによる権利処理後のコンテンツの再生信号を、該当する権利管理・保護方式の仕様記述に従ってＡＰＳ（Analog Protection System）処理して外部出力する外部出力ステップを備えていてもよい。

【0044】また、前記権利処理ステップによる権利処

理後のコンテンツを暗号化して外部出力する外部出力ステップを備えていてもよい。

【００４５】また、本発明の第３の側面は、所定の権利管理・保護（Right Management & Protection：ＲＭＰ）方式に則って配信されるコンテンツの受信処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、配信コンテンツを受信するコンテンツ受信ステップと、受信コンテンツの権利管理・保護方式を識別する識別ステップと、前記識別ステップによる識別結果に基づいて、該当する権利管理・保護方式に従って受信コンテンツを権利処理する権利処理ステップと、を具備することを特徴とする記憶媒体である。

【００４６】本発明の第３の側面に係る記憶媒体は、例えば、様々なプログラム・コードを実行可能な汎用性のコンピュータ・システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で物理的に提供する媒体である。このような媒体は、例えば、ＣＤ（Compact Disc）やＦＤ（Floppy Disc）、ＭＯ（Magneto-Optical disc）などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを経由してコンピュータ・ソフトウェアを特定のコンピュータ・システムにコンピュータ可読形式で提供することも技術的に可能である。

【００４７】このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、本発明の第３の側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１及び第２の各側面に係るコンテンツ受信装置及びコンテンツ受信方法と同様の作用効果を得ることができる。

【００４８】また、本発明の第４の側面は、それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、権利管理・保護方式の識別情報を含んだ要求に応答して、該当する権利管理・保護モジュールを送信する手段と、を備えることを特徴とするサーバである。

【００４９】また、本発明の第５の側面は、それぞれの権利管理・保護方式に対応した複数の権利管理・保護モジュールを蓄積する手段と、識別情報に基づく問合せに応答して、該当する権利管理・保護モジュールを用いてコンテンツを変換する手段と、を具備することを特徴とするサーバである。

【００５０】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００５１】

【発明の実施の形態】以下に記述する本発明の実施形態では、各コンテンツ配信システム毎に策定される複数のＲＭＰに対応することができるコンテンツ受信装置について説明する。

【００５２】ＲＭＰは、Right Management & Protectionの略であり、ＴＶ Ａｎｙｔｉｍｅ Ｆｏｒｕｍで用いられている概念である。放送やネットワークを介したコンテンツ配信事業において問題になるのが、コンテンツの不正利用やタダ見、タダ聴きである。この種の不正行為が横行すると、コンテンツ制作・提供・配信事業者の正当な利益が保証されず、事業の存亡にも関わる。言い換えれば、コンテンツの利用権利管理と保護が必要であり、ＲＭＰがこれを担う。

【００５３】ＲＭＰには、より具体的には、暗号化の方式、鍵の配布方式、コンテンツ暗号解読方式、課金情報や鍵類の伝送方式、記録メディア制御情報、相互認証の方式、ＡＰＳ（Analog Protection System：マクロビジョンやＣＧＭＳ（Copy Generation Management System）など）、視聴制限情報などの、コンテンツ購入とコンテンツ利用に必須の項目が含まれている。

【００５４】これらの項目からなるＲＭＰの仕様を規定する書式のみを統一化し、各コンテンツ提供事業者は該仕様に則った形式で暗号化コンテンツや権利処理情報をコンテンツに入力すればよい。このような場合、コンテンツを受信し利用する消費者すなわちコンテンツ利用者側では、各々のＲＭＰ方式に対応した機能を複数用意しておくことにより、どのようなＲＭＰ方式に基づくコンテンツであっても、同じコンテンツ受信機上で復号化して利用に供することができる。

【００５５】ＲＭＰ仕様記述は、例えば、配信コンテンツに付随するメタデータの一部として記述することができる。以下では、メタデータのうちＲＭＰ仕様記述に関連する部分のことを「権利処理メタデータ」と呼ぶことにする。例えば、デジタル放送などの場合、放送番組本編に付随するデータ放送用データとしてメタデータを配信することができる。

【００５６】図１には、ＲＭＰモジュールの概念構成を示している。ＲＭＰモジュールは、例えば、ＳＴＢ（Set Top Box）やその他の形態のコンテンツ受信機に内蔵して用いられ、所定のハードウェア又はソフトウェアのモジュールを用いて実装することができる。同図に示すように、ＲＭＰモジュールは、受信コンテンツに関するデータを入出力を行うための幾つかのインターフェースを備えた構成となっている。

【００５７】衛星波又は地上波などの放送を介して受信されたコンテンツ、あるいは、インターネットなどのネットワーク経由でダウンロードされたコンテンツは、メ

タデータとともに、ハード・ディスク装置などのような大容量蓄積装置内に格納される。RMPモジュールは、ハード・ディスク装置経由で、あるいはハード・ディスク装置を介さずに直接、権利処理前の状態で受信コンテンツを入力する。

【0058】映像や音楽などのコンテンツ本体はコンテンツ保護の目的で暗号化が施されている。したがって、暗号化コンテンツを解くための解読機能（Decryptor）が必要であり、RMPモジュールは、規定された暗号アルゴリズムにより暗号化コンテンツを入力する暗号化コンテンツ入力用インターフェースを持つ。

【0059】また、各コンテンツに対応してメタデータが配信されるが、その中には、コンテンツに関する権利処理や必要な権利保護を示す情報、すなわち権利処理メタデータが含まれている。

【0060】権利処理メタデータには、コンテンツを解くための鍵類、コンテンツの購入条件、使用条件、解読されたコンテンツのコピー制御情報などが含まれる。RMPモジュールは、規定のフォーマットに従い権利処理や保護に関する情報を入力する権利処理メタデータの入力インターフェースを持つ。

【0061】配信コンテンツは、例えばコンテンツ鍵によって暗号化され、このコンテンツ鍵はさらに配信鍵（Distribution Key）によって暗号化された形態で、暗号化コンテンツとともに伝送されてくる。RMPモジュール内には配信鍵が保持されており、この配信鍵を用いて暗号化されたコンテンツ鍵を解読し、さらに、解読されたコンテンツ鍵を用いて暗号化コンテンツを解読することができる。このような暗号化・伝送方式によれば、コンテンツ毎にコンテンツ鍵を変えながら安全にコンテンツ配信を行うことができるとともに、RMPモジュールでは単一の配信鍵を保持することで暗号化コンテンツを解読して利用に供することができる。RMPモジュールの権利処理メタデータ入力インターフェースは、暗号化コンテンツ鍵を権利処理メタデータとして入力するようにしてもよい。

【0062】また、コンテンツ制作・提供事業者において策定するコンテンツ利用のための課金に関する仕様も、権利処理メタデータに含め、RMPモジュールの権利処理メタデータ入力インターフェースはこれを入力するようにしてもよい。

【0063】課金に関する仕様として、例えば、価格情報、使用条件（1回毎の再生課金、あらかじめ再生可能な回数を規定した回数制限、所定の期日まで再生可能とした期間制限など）などを規定することができる。

【0064】コンテンツ利用者に対する課金処理のために、管理センタのようなコンテンツ制作・提供・配信事業者以外の決済機関を設立してもよい。RMPモジュールは、このような管理センタに接続して、課金や決済に関するトランザクションを行うための課金処理インターフェースを持つ。RMPモジュールは、例えば、ハード・ディスク装置上に蓄積されたコンテンツを再生する毎に課金ログを生成して、所定期間毎に管理センタに接続してログを送信する。これに対し、管理センタは、各コンテンツ利用者から送られてくるログに基づいて課金並びに決済処理を行うことができる。

【0065】RMPモジュールは、権利処理前の受信コンテンツを入力するための暗号化コンテンツ用インターフェースを備えていることは既に述べた通りである。RMPモジュールは、コンテンツの数回にわたる利用のために、権利処理後のコンテンツを再びハード・ディスク装置に蓄積するためのインターフェースや、コンテンツの永久・半永久保存のために、権利処理後のコンテンツをDVD（Digital Versatile Disc）などのリムーバブル・メディア上に格納するためのインターフェースを備えている。このような権利処理後のコンテンツ蓄積・再生用のインターフェースは、蓄積用コンテンツの暗号化や再生時における復号化などのメディアに対する制御や、メディアに対する認証の有無や認証方法などを規定することができる。

【0066】また、RMPモジュールは、受信コンテンツ、あるいはハード・ディスク装置やリムーバブル・メディアから読み出したコンテンツを、ディスプレイやその他の外部機器で再生するための外部出力インターフェースを備えている。図1に示す例では、ビデオ信号としてディスプレイ上に表示出力するためのアナログ出力インターフェースと、IEEE 1394などのホームネットワーク経由で外部機器にコンテンツを転送するためのデジタル出力インターフェースを備えている。アナログ出力インターフェースは、アナログ形式のコンテンツ保護のために、APS（Analog Protection System）などを採用する。APSには、マクロビジョンや、垂直帰線区間の所定の走査線にコピー制御情報を埋め込むCGMS（Copy Generation Management System）-A、SCMSなどが含まれる。また、デジタル出力インターフェースでは、送信コンテンツ暗号化の他、1394CPのような認証バス・エンクリプションなどの制御を行うことができる。

【0067】また、権利処理後のコンテンツを転送して、パーソナル・コンピュータ（PC）のような情報処理機器上で所望のアプリケーションを用いた処理を行うことができる。図1に示す例では、RMPモジュールは、外部の情報処理機器にコンテンツを出力するためのホスト/アプリケーション用インターフェースを備えている。ホスト/アプリケーション用インターフェースは、送信コンテンツの暗号化などの制御を行う。

【0068】RMPモジュールは、専用のハードウェア・コンポーネントで実装することも、あるいは、汎用プロセッサ上で所定のプログラム・コードを実行することによっても実現可能である。RMPに関する仕様は、権

利処理メタデータとして、配信コンテンツに付随して配信・配布することができる（前述）。

【0069】RMP仕様記述フォーマットの一例を以下に示しておく。

【0070】

【数1】


```
RMP ID::=INTEGER{XXXXXXX}
Contents Encription Algorithm::=SEQUENCE{
    algorithm               3DES
    developper              Public
    download                URL

    key length              112
    key parity              16
    key name                Content Key
}
Content Key Encryption Algorithm::=SEQUENCE{
    algorithm               DES
    developper              Public
    download                URL
    key length              56
    key parity              8
    key name1               Distribution Key
    key name2               Storage Key
}
Distribution Key Encryption Algorithm::=SEQUENCE{
    algorithm               None
}
Storage Key Encryption Algorithm::=SEQUENCE{
    algorithm               None
}
Authentication Algorithm::=SEQUENCE{
    algorithm               DES
    developper              Public
    download                URL
    ECC parameter p         xxxxxxxxxxxxxxxx
    ECC parameter a         xxxxxxxxxxxxxxxx
    ECC parameter b         xxxxxxxxxxxxxxxx
    ECC parameter g         xxxxxxxxxxxxxxxx
    ECC parameter r         xxxxxxxxxxxxxxxx
    key length              224

    key party               0
}
Log Format::=SEQUENCE{
    log serial number       xxxxxxxx
    purchase date           yyyy:mm:dd
    purchase time           hh:mm:ss
    content ID              xxxxxxxxxx
    purchase condition      xxx
    purchase limitation     xxxxxx
    purchase price          xxxxxx
    copy permission         xx
}
    ... ... ... ... ... ...
```

【0071】上記で示したRMP仕様記述フォーマット

では、RMPの方式を識別するための識別情報（RMP ID）を冒頭に含む他、配信コンテンツを暗号化する暗号化アルゴリズム、配信コンテンツの暗号化に使用するコンテンツ・キーKsを暗号化する暗号化アルゴリズム、コンテンツ配信時に使用する配信キーKdを暗号化する暗号化アルゴリズム、配信コンテンツを蓄積するときに使用するストレージ・キーKst、相互認証に用いる認証アルゴリズム、ログを蓄積するためのフォーマットなどを規定することができる。暗号化方式としては、一般に、DES（Data Encription Standard）やMulti2などが使用される。

【0072】RMPとしての仕様記述は、各コンテンツ制作・提供事業者毎に策定される。従来は、各コンテンツ配信システム毎にRMPを固定して利用していたので、複数のシステムからコンテンツの提供を受けるためには、新しいコンテンツ受信機を用意するなど余計な出費が必要であった。これに対し、本発明では、RMPの仕様記述、並びにRMPに入力するためのインターフェースを規定することにより、その仕様を解読するか、又はその仕様に適合したRMPモジュールを入手することにより、同一のコンテンツ受信機上で、複数のコンテンツ配信システムにおけるコンテンツ課金、暗号化などのセキュリティ方式、著作権保護方式に対応することができる。

【0073】本発明の1つの実現形態としては、コンテンツ受信機あるいはコンテンツ記録再生機内で、異なるRMP仕様を実装した複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用することが挙げられる。

【0074】また、他の実現形態として、ソフトウェア・モジュールとしてRMPモジュールを構成し、各受信コンテンツ毎に適合するソフトウェア・モジュールを所定のサーバからダウンロードすることや、あるいは権利処理メタデータを解析して、所望のソフトウェア・モジュールをコンテンツ受信機側で自動生成することが挙げられる。

【0075】図2には、異なるRMP仕様を実装した複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用する形式のコンテンツ受信機10の構成を模式的に図解している。

【0076】同図に示すコンテンツ受信機10は、フロント・エンド部11と、CAS処理部12と、コンテンツ蓄積用のハード・ディスク装置13A並びに13Bと、RMP識別部14と、それぞれ異なるRMP仕様記述に基づく2つ（複数）のRMPモジュール1並びにRMPモジュール2とで構成される。

【0077】フロント・エンド部11は、所定チャネルの放送波のチューニングすなわち選局処理と、受信データの復調処理を行う。

【0078】CAS処理部12は、コンテンツ配信事業者との間で交わされたCAS（Conditional Access System（限定受信））に関する契約に基づき、放送コンテンツに適用されたスクランブル処理の解除（デスクランブル）を行う。日本国内のデジタル放送では、BS、CSともに共通の"MULTI2"と呼ばれるスクランブル方式を採用する。但し、CAS処理自体は本発明の要旨に関連しないので、ここではこれ以上説明しない。

【0079】ハード・ディスク装置13A及び13Bは、受信コンテンツの蓄積に使用される。より具体的には、一方のハード・ディスク装置13AはRMPモジュールによる権利処理前の状態のコンテンツの蓄積に使用され、他方のハード・ディスク装置13Bは権利処理後の状態のコンテンツの蓄積に使用される。但し、ハード・ディスク装置13A及び13Bは、物理的に互いに独立した装置である必要はなく、例えば、単一のハード・ディスク上に割り当てられた別個の記憶領域（パーティション）であってもよい。

【0080】本実施例では、権利処理メタデータの一部として記述されるRMPには、その方式を識別するための固有の識別情報（RMP ID）が割り振られている。RMP識別部14は、ハード・ディスク装置13Aから権利処理メタデータを読み出して、RMP IDを識別して、2つ（複数）のRMPモジュール1並びにRMPモジュール2のうち識別されたRMP IDに対応する方を動作可能にする。

【0081】RMPモジュール1並びにRMPモジュール2は、暗号化された映画や音楽などのコンテンツ、並びにコンテンツに付随する権利処理メタデータを処理するための幾つかのインターフェース（前述）を備えている。RMP識別部14により付勢されたRMPモジュール1又はRMPモジュール2は、権利処理メタデータとして記述されたRMP仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置13Bやリムーバブル・メディアへの格納などのコンテンツ処理を行う。

【0082】また、図3には、他の実施形態に係るコンテンツ受信機20の構成を模式的に図解している。コンテンツ受信機20は、異なるRMP仕様を実装した複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用するようになっている。

【0083】同図に示す例では、コンテンツ受信機20は、フロント・エンド部21と、ハード・ディスク装置23と、RMP識別部24と、各RMPモジュール1及びRMPモジュール2と、デコーダ出力装置25が、同一のデータ・バス26を介して相互接続された構成となっている。

【0084】フロント・エンド部21は、所定チャネル

の放送波のチューニングすなわち選局処理と、受信データの復調処理を行う。但し、図示しないが、放送波を介さない代わりに、インターネットなどの広域ネットワーク経由で所定のサービス・プロバイダからコンテンツを受信する場合においては、フロント・エンド部21は、ネットワーク・インターフェース・カードで実現することができる。

【0085】ハード・ディスク装置23は、RMPモジュールによる権利処理前の状態のコンテンツを蓄積したり、権利処理後の状態のコンテンツを蓄積するために使用される。

【0086】権利処理メタデータとして記述されるRMPには、その方式を識別するための固有の識別情報RMP IDが割り振られている。RMP識別部24は、ハード・ディスク装置23から権利処理メタデータを読み出して、RMP IDを識別して、2つ（複数）のRMPモジュール1並びにRMPモジュール2のうち識別されたRMP IDに対応するものを動作可能にする。

【0087】RMPモジュール1並びにRMPモジュール2は、暗号化された映画や音楽などのコンテンツ、並びにコンテンツに付随する権利処理メタデータを処理するための幾つかのインターフェース（前述）を備えている。RMP識別部24により付勢されたRMPモジュール1又はRMPモジュール2は、権利処理メタデータとして記述されたRMP仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置23やリムーバブル・メディアへの格納などのコンテンツ処理を行う。なお、CAS方式を採用するコンテンツ配信事業者からコンテンツを受信する場合には、対応する暗号解読・デスクランブル処理を行うCASモジュールをRMPモジュール上に搭載するようにしてもよい。

【0088】デコーダ出力装置25は、権利処理後の再生コンテンツのデコード処理並びに外部出力を行う。例えば、AVコンテンツであれば、デコーダ出力装置25は、コンテンツを圧縮映像データと圧縮音声データに分離処理する。そして、MPEG2などによる圧縮映像データを伸張処理して、元のビデオ信号を再生するとともに、圧縮音声データに関しては、PCM（Pulse Code Modulation）デコードした後に付加音と合成して再生音声信号とする。

【0089】また、図4には、他の実施形態に係るコンテンツ受信機30の構成を模式的に図解している。コンテンツ受信機30は、ソフトウェア・モジュールとしてRMPモジュールを構成し、各受信コンテンツ毎に適合するソフトウェア・モジュールを所定のサーバからダウンロードするようになっている。

【0090】同図に示すように、コンテンツ受信機30は、フロント・エンド部31と、CPU（Central Processing Unit）32と、ハード・ディスク装置33A及び33Bと、RMP識別部34と、作業メモリ35と、デコーダ出力装置36と、ネットワーク・インターフェース37が、システム・バス38を介して相互接続された構成となっている。

【0091】フロント・エンド部31は、所定チャネルの放送波のチューニングすなわち選局処理と、受信データの復調処理を行う。

【0092】ネットワーク・インターフェース37は、TCP／IP（Transmission Control Protocol/Internet Protocol）などの所定の通信プロトコルに従ってコンテンツ受信機37をインターネットなどの広域ネットワークに接続するための装置である。インターネット上には無数のホスト端末が接続されている。ホスト端末の一部は、映画や音楽などのコンテンツを配信する情報配信サーバであり、他の一部はソフトウェアRMPモジュールを配信するサーバである。なお、放送経由でコンテンツを受信する代わりに、インターネットなどの広域ネットワーク経由で所定のサービス・プロバイダからコンテンツを受信する場合においては、フロント・エンド部31は、ネットワーク・インターフェース37によって実現することができる。

【0093】CPU32は、オペレーティング・システム（OS）の制御下で、コンテンツ受信機30内の動作を統括的に制御する中央コントローラであり、作業メモリ35を用いて各種のプログラム・コードを実行する。

【0094】ハード・ディスク装置33Aは、RMPモジュールによる権利処理前の状態でのコンテンツの蓄積、並びに、権利処理後の状態のコンテンツの蓄積に使用される。また、ハード・ディスク装置33Bは、以前使用した（あるいはあらかじめダウンロードしておいた）ソフトウェアRMPモジュールの蓄積に利用される。ハード・ディスク装置33Aと33Bは、それぞれ独立した装置ユニットである必要はなく、例えば単一のハード・ディスク装置上で区切られた記憶領域（例えばパーティション）であってもよい。

【0095】権利処理メタデータとして記述されるRMPには、その方式を識別するための固有の識別情報RMP IDが割り振られている。RMP識別部34は、ハード・ディスク装置33から権利処理メタデータを読み出して、RMP IDを識別して、該当するソフトウェアRMPモジュールが作業メモリ35上にロードされて現在使用中か否かを検出する。RMP識別部34は、ハードウェア・コンポーネントとしてではなく、CPU32が実行するプログラム・コードとして実装することもできる。

【0096】作業メモリ35上のソフトウェアRMPモジュールが、これから再生するコンテンツに関するRMP IDにヒットしない場合には、該当するソフトウェアRMPモジュールをローカル・ディスク33B上で探索し、見つかった場合にはこれを作業メモリ35上のも

のと置き換える。ローカル・ディスク３３Ｂ上で該当するソフトウェアＲＭＰモジュールを発見することができなかった場合には、さらに、ネットワーク・インターフェース３７経由でネットワーク上のサーバにアクセスして、所望のソフトウェアＲＭＰモジュールを探索することができる。

【００９７】ＣＰＵ３２は、作業メモリ３５上にロードされたソフトウェアＲＭＰモジュールを実行することにより、権利処理メタデータとして記述されたＲＭＰ仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置３３Ａやリムーバブル・メディアへの格納などのコンテンツ処理を行うことができる。なお、ＣＡＳ方式を採用するコンテンツ配信事業者からコンテンツを受信する場合には、対応する暗号解読・デスクランブル処理を行うＣＡＳモジュールを同様に作業メモリ３５上にロードすればよい。

【００９８】デコーダ出力装置３６は、権利処理後の再生コンテンツのデコード処理並びに外部出力を行う。例えば、ＡＶコンテンツであれば、デコーダ出力装置３６は、コンテンツを圧縮映像データと圧縮音声データに分離処理する。そして、ＭＰＥＧ２などによる圧縮映像データを伸張処理して元のビデオ信号を再生するとともに、圧縮音声データに関してはＰＣＭ（Pulse Code Modulation）デコードした後に付加音と合成して再生音声信号とする。

【００９９】図５には、コンテンツ受信機３０にソフトウェアＲＭＰモジュールをダウンロードするための処理手順をフローチャートの形式で示している。以下、このフローチャートに従って、ソフトウェア・モジュールのダウンロード処理について説明する。

【０１００】ハード・ディスク装置３３Ａに蓄積しておいたコンテンツの再生を開始する際、対応する権利処理メタデータを同様にハード・ディスク装置３３Ａから読み出して、ＲＭＰモジュールのＲＭＰ　ＩＤを取得する（ステップＳ１）。そして、このＲＭＰ　ＩＤが現在作業メモリ３５にロードされているＲＭＰモジュールのそれと一致するか否かをチェックする（ステップＳ２）。

【０１０１】ＲＭＰ　ＩＤがヒットする、すなわち、これから再生するコンテンツのＲＭＰモジュールが既に作業メモリ３５上にロードされている場合には、続いて管理センタと接続確立して、ＲＭＰ仕様記述に基づいてコンテンツ購入に関する課金処理を行った後（ステップＳ３）、コンテンツ再生を行い（ステップＳ４）、本処理ルーチン全体を終了する。

【０１０２】他方、ＲＭＰ　ＩＤがヒットしなかった場合には、ＲＭＰ入手先情報を取得して（ステップＳ５）、ＲＭＰ入手先となるサーバに接続して（ステップＳ６）、該当するソフトウェアＲＭＰモジュールをこのサーバからダウンロードする（ステップＳ７）。そして、ダウンロードしたソフトウェアＲＭＰモジュールをコンテンツ受信機３０にインストール（例えば、作業メモリ３５上にロード）する（ステップＳ８）。

【０１０３】ＲＭＰ入手先情報は、例えば権利処理メタデータ内にＵＲＬ（Uniforn Resource Locator）形式で記述されている。このような場合、コンテンツ受信機３０は、ネットワーク・インターフェース３７経由でインターネットのようなＴＣＰ／ＩＰネットワーク経由でＵＲＬで指示されたサーバに対し資源アクセスして、該当するＲＭＰモジュールをＨＴＴＰ（Hyper Text Transfer Protocol）又はＦＴＰ（File Transfer Protocol）などの転送プロトコルに従ってダウンロードすることができる。

【０１０４】新規のソフトウェアＲＭＰモジュールをインストールした結果、コンテンツ受信機３０上において、権利処理メタデータとして記述されたＲＭＰ仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置３３Ａやリムーバブル・メディアへの格納などのコンテンツ処理を行うことができるようになる。

【０１０５】続いて、管理センタと接続確立して、ＲＭＰ仕様記述に基づいてコンテンツ購入に関する課金処理を行った後（ステップＳ３）、コンテンツ再生を行い（ステップＳ４）、本処理ルーチン全体を終了する。

【０１０６】ソフトウェア・モジュールとしてＲＭＰモジュールを構成する変形例として、ＣＰＵ３２（あるいは他の演算処理ユニット）が権利処理メタデータ内のＲＭＰ仕様記述を解析して、所望のソフトウェアＲＭＰモジュールをコンテンツ受信機３０内部で自動生成するようにしてもよい。

【０１０７】図６には、ソフトウェアＲＭＰモジュールをコンテンツ受信機３０内部で自動生成するための処理手順をフローチャートの形式で図解している。以下、このフローチャートに従って、ソフトウェアＲＭＰモジュールの自動生成処理について説明する。

【０１０８】ハード・ディスク装置３３Ａに蓄積しておいたコンテンツの再生を開始する際、対応する権利処理メタデータを同様にハード・ディスク装置３３Ａから読み出して、ＲＭＰモジュールのＲＭＰ　ＩＤを取得する（ステップＳ１１）。そして、このＲＭＰ　ＩＤが現在作業メモリ３５にロードされているＲＭＰモジュールのそれと一致するか否かをチェックする（ステップＳ１２）。

【０１０９】ＲＭＰ　ＩＤがヒットする、すなわち、これから再生するコンテンツのＲＭＰモジュールが既に作業メモリ３５上にロードされている場合には、続いて管理センタと接続確立して、ＲＭＰ仕様記述に基づいてコンテンツ購入に関する課金処理を行った後（ステップＳ１３）、コンテンツ再生を行い（ステップＳ１４）、本処理ルーチン全体を終了する。

【0110】他方、RMP IDがヒットしなかった場合には、RMP仕様記述に関する情報を権利処理メタデータから取得する（ステップS15）。次いで、コンテンツ受信機30上のコンピューテーション・パワー（例えば、CPU32が持つ計算能力）がRMPモジュールを生成するに足りるか否かをチェックする（ステップS16）。

【0111】コンピューテーション・パワー不足の場合には、コンテンツの再生が不可である旨のメッセージを表示した後（ステップS19）、本処理ルーチンを異常終了する。

【0112】他方、コンピューテーション・パワーが充分であった場合には、さらに、RMP仕様記述を解読して（ステップS17）、作業メモリ35上でRMPを設定する（ステップS18）。新規にRMPを設定した結果、コンテンツ受信機30上において、権利処理メタデータとして記述されたRMP仕様記述通りに動作して、暗号化コンテンツの復号化、再生コンテンツとしての外部出力、ハード・ディスク装置33Aやリムーバブル・メディアへの格納などのコンテンツ処理を行うことができるようになる。

【0113】続いて、管理センタと接続確立して、RMP仕様記述に基づいてコンテンツ購入に関する課金処理を行った後（ステップS13）、コンテンツ再生を行い（ステップS14）、本処理ルーチン全体を終了する。

【0114】なお、ハードウェア・モジュールとしてRMPモジュールを構成した場合、ソフトウェアによりモジュールを実装する場合に比し、簡単に他のRMPモジュールに置き換えることはできない。このような場合、サーバ側において、受信機に対応したRMPに置き換えるような仕組みを提供してもよい。例えば、コンテンツ受信機側は、コンテンツのIDでサーバに問い合わせて、コンテンツの変換を依頼する。権利処理条件が整っていれば、所定のRMPに変換することができ、変換後のコンテンツ（あるいは、あらかじめ同じコンテンツが用意されていることでもよい）を依頼元のコンテンツ受信機にダウンロードすることで、希望するコンテンツの復号化・再生を実現することができる。

【0115】次いで、コンテンツ・プロバイダが衛星放送を利用してコンテンツ配信を行うコンテンツ配信システムに対して本発明を適用した場合の実施例について説明する。

【0116】図7には、コンテンツ配信システム100の概略的構成を図解している。同図に示すコンテンツ配信システム100は、コンテンツを制作・提供する番組制作会社又は委託放送事業者からなるコンテンツ・プロバイダ200と、制作・提供されたコンテンツを衛星放送波によって配信する衛星放送受託放送事業者（以下、単に「放送局」とする）300と、各一般家庭などに設置されたコンテンツ配信対応衛星放送受信機（以下、単

に「コンテンツ受信機」とする）400とで構成される。コンテンツ受信機400は、一般に、映像及び音声出力用のテレビジョン（TV）450と接続されている。

【0117】コンテンツ・プロバイダ200と放送局300との間では、コンテンツ制作・提供に関する委託契約が交わされており、コンテンツ・プロバイダ200が制作（あるいは外部のコンテンツ・プロバイダから取得した）コンテンツは放送局300に提供される。放送局300は、コンテンツを暗号化して、これを衛星放送波にのせて各家庭内のコンテンツ受信機400に向けて配信する。

【0118】コンテンツ・プロバイダ200は、コンテンツ制作事業者としての番組制作会社201とは独立した、コンテンツ課金を管理する外部の管理センタ202のような決済専門の機関と契約していてもよい。このような場合、コンテンツ・プロバイダ200はコンテンツを暗号化する鍵の管理を管理センタ202に委ね、管理センタ202はコンテンツ販売情報を渡す。

【0119】管理センタ201は、さらに外部の認証局250や他の決済機関と連動していてもよい。また、管理センタ202は、個々のコンテンツ受信機400との間で定期的あるいは不定期的に接続され、コンテンツ受信機400に対して暗号化コンテンツを利用可能にするための鍵情報を配布する。コンテンツ受信機400は、配布された鍵情報を用い、RMP仕様記述に基づいて、放送衛星301経由で受信した暗号化コンテンツを解読して利用に供する。また、コンテンツ受信機400は、ハード・ディスク装置のような大容量外部記憶装置を内蔵しており、受信したコンテンツを蓄積することができる。

【0120】また、コンテンツ受信機400から管理センタ201に対しては、コンテンツの再生ログなど課金情報が送られてくる。コンテンツ受信機400側のユーザは、例えば、コンテンツ使用回数相当の課金額を管理センタに対して月々決済すればよい。決済方法は、現金納付、所定の金融機関への振り込み、プリペイド・カードによる予納、クレジット・カードによる信用決済、デビット・カードによる即時決済、電子マネーの利用などいずれでもよい。

【0121】図8には、コンテンツ制作並びに配信を行う放送局300における構成を模式的に図解している。以下、図8を参照しながら、コンテンツ配信時における暗号化などの仕組みについて説明する。

【0122】コンテンツ暗号化部311は、コンテンツ・プロバイダから提供された映像や音楽などのコンテンツを、コンテンツ鍵（コンテンツ・キー）Kcを用いて暗号化する。但し、コンテンツ・プロバイダから提供されるコンテンツは、コンテンツ・プロバイダにおいて策定されたRMP仕様記述に則った暗号化その他の権利処

理が適用されているものとする。

【0123】コンテンツ鍵暗号化部312は、配信鍵（ディストリビューション・キー）KDを用いてコンテンツ鍵Kcを暗号化する。

【0124】マルチプレクサ313は、コンテンツ暗号化部311から入力する暗号化コンテンツと、コンテンツ鍵暗号化部312から入力する暗号化コンテンツ鍵を多重化して、トランスポート・ストリームTS（Transport Stream）を生成する。トランスポート・ストリームは、暗号化コンテンツにメタデータや、暗号化コンテンツ鍵が付加されたデータ・ストリームである。

【0125】CASスクランブラ314は、コンテンツ受信機400において限定受信させるべく、トランスポート・ストリームをスクランブルすなわち攪拌処理する。CASにおける契約情報やスクランブル鍵などは、例えば図示しない暗号化装置により暗号化され、放送波にのせてコンテンツ受信機400側に送信することができる。

【0126】図9には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機の一例400Aの構成を模式的に示している。同図に示すコンテンツ受信機400Aは、受信したコンテンツをハード・ディスクなどの所定のローカル記憶装置に一旦蓄積した後でコンテンツの購入を決定するタイプである。以下、同図を参照しながらコンテンツ受信機400Aについて説明する。

【0127】CASデスクランブラ411は、図示しないフロント・エンドにより受信されたデータを、放送局300側から取得したスクランブル鍵を用いてデスクランブルして、トランスポート・ストリームを再現する。

【0128】デマルチプレクサ412は、トランスポート・ストリームを、暗号化コンテンツと暗号化コンテンツ鍵とに分離する。分離後、これらは権利処理前の状態のままハード・ディスク装置413Aに一旦蓄積される。

【0129】RMPモジュール420は、ハードウェア・モジュールあるいはソフトウェア・モジュールいずれの形態で実装されていてもよい。ハード・ディスク装置413Aに蓄積したコンテンツを購入する際、まず、対応する権利処理メタデータが読み出され、その中からRMP識別情報（RMP ID）が検出され、適当なRMPモジュールが選択的に動作しているものとする。

【0130】RMPモジュール420は、コンテンツ購入に関する契約を交わした（あるいはユーザ・アカウントを取得している）管理センタ202と接続して、コンテンツの配信鍵KDを購入する。コンテンツ鍵復号化部421は、権利処理メタデータから暗号化コンテンツ鍵を取り出して、これを配信鍵KDで復号化してコンテンツ鍵Kcを得る。後続のコンテンツ鍵再暗号化部422は、RMPモジュール420で規定されているコンテンツ蓄積用の鍵（ストレージ・キー）Ksを用いてコンテンツ鍵Kcを再暗号化する。

【0131】購入した暗号化コンテンツを、再暗号化されたコンテンツ鍵とともに、ハード・ディスク装置413Aからハード・ディスク装置413Bに移動する。但し、ハード・ディスク装置413Aと413Bは、物理的に独立した装置ユニットである必要はなく、同一のハード・ディスク内で権利処理前（購入前）と権利処理後（購入後）とで記憶領域（例えば、パーティション）を区切られたものであってもよい。

【0132】RMPモジュール420は、購入コンテンツのための配信鍵KDの購入や、購入コンテンツの移動などの処理ログを、課金データとして蓄積しておく。そして、定期的あるいは不定期的に管理センタ202に接続して、課金データを転送する。

【0133】また、図10には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例400Bの構成を模式的に示している。同図に示すコンテンツ受信機400Bは、受信したコンテンツを一旦ハード・ディスクなどのローカル記憶装置に蓄積した後、コンテンツを再生を行うタイプである。コンテンツ受信機400Bは、上述したコンテンツ受信機400Aにより購入・蓄積された暗号化コンテンツの再生装置としても機能する。以下、同図を参照しながらコンテンツ受信機400Bについて説明する。

【0134】ハード・ディスク装置433内には、RMPモジュール440で規定されたコンテンツ鍵Kcを用いて暗号化されたコンテンツと、RMPモジュール440で規定されているコンテンツ蓄積用の鍵（ストレージ・キー）Ksで暗号化された暗号化コンテンツ鍵が格納されている。

【0135】コンテンツ購入時には、コンテンツ鍵復号化部441は、ハード・ディスク装置433から該当する暗号化コンテンツ鍵を読み出して、これを規定された格納鍵Ksを用いて復号化して、コンテンツ鍵Kcを得る。

【0136】コンテンツ復号化部442は、購入したい暗号化コンテンツをハード・ディスク装置433から読み出して、これを復号化されたコンテンツ鍵Kcを用いて復号化し、元の映像又は音楽などのコンテンツを再現する。

【0137】APS処理部443は、ビデオ信号などのアナログ出力信号に対して、マクロビジョンやCGMS-Aなどのコンテンツ保護処理を適用した後、再生コンテンツとしてテレビジョン（図示しない）などの出力装置に送出する。

【0138】図9及び図10に示すようなコンテンツ受信機400Aによれば、コンテンツ・プロバイダは、CASとは独立した暗号化システムによりコンテンツを配信することができる。すなわち、CASに依存しないコ

ンテンツ配信システムなので、異なるＣＡＳ（異なる放送事業者）にまたがった共通のプラットフォーム上でコンテンツ購入に対する課金処理を行うことができる。この場合、ＣＡＳは、単なるコンテンツの流通経路に過ぎない。コンテンツは暗号化されたままの状態でハード・ディスク装置のようなローカル記憶装置に蓄積される。購入時に、コンテンツを解くための鍵がコンテンツ鍵Ｋｃから格納鍵Ｋｓにかけ変えられるので、その後は同じコンテンツ受信機４００Ａ上でいつでも再生することができる。また、コンテンツ購入処理時に課金するためのログが作成され、定期的あるいは不定期的に管理センタ２０２に送信されるので、コンテンツ利用者に対して確実に課金・決済を行うことができる。

【０１３９】図１１には、図９に示したようなコンテンツ受信機４００Ａにおいて、受信コンテンツをハード・ディスク装置４１３Ａに蓄積するための処理手順の一例をフローチャートの形式で示している。受信コンテンツは、基本的には、権利処理前のまま蓄積される。以下、このフローチャートに従って、コンテンツの蓄積処理について説明する。

【０１４０】まず、コンテンツ受信機４００Ａのユーザにより予約したい番組が決まっているか否か（すなわち予約設定されているか否か）をチェックする（ステップＳ２１）。

【０１４１】予約したい番組が既に決められている場合には、例えばデジタル放送であればデータ放送用データの中からＥＰＧ（Electric Program Gulde：電子番組表）を取り出し、ＥＰＧを基に予約すべき番組を選択する（ステップＳ２２）。そして、予約すべき時刻（放映時間帯）並びにチャンネルなどを設定する（ステップＳ２３）。

【０１４２】次いで、ユーザからのプリファレンス入力（ステップＳ２４）を基に、プリファレンスにあった番組を所定の検索エンジンが自動選択する（ステップＳ２５）。そして、予約すべき時刻（時間帯）並びにチャンネルなどを設定する（ステップＳ２６）。

【０１４３】予約開始時刻に到達した、あるいは選択された番組ＩＤが受信されたことに応答して、ハード・ディスク装置への受信コンテンツの自動蓄積を行う（ステップＳ２７）。

【０１４４】また、図１２には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例４００Ｃの構成を模式的に示している。同図に示すコンテンツ受信機４００Ｃは、ＩＣカード化された衛星放送用のＣＡＳモジュール、すなわちＢＳ－ＣＡＳ ＩＣカードを内蔵しており、受信したコンテンツを一旦ハード・ディスク装置に蓄積した後、ＣＡＳシステムに基づいて衛星放送を限定受信して視聴するタイプである。以下、同図を参照しながら、コンテンツ受信機４００Ｃについて説明する。

【０１４５】図示しないフロント・エンドにより受信されたデータ・コンテンツは、権利処理前で且つＣＡＳによりスクランブル処理された状態のまま、ハード・ディスク装置４５３のような大容量記憶装置に一時蓄積される。

【０１４６】受信コンテンツの権利処理はＲＭＰモジュール４６０により行われる。ＲＭＰモジュール４６０は、ハードウェア・モジュールあるいはソフトウェア・モジュールいずれの形態で実装されていてもよい。ハード・ディスク装置４５３に蓄積したコンテンツを購入する際、対応する権利処理メタデータが読み出され、ＲＭＰ識別情報（RMP ID）が検出され、適当なＲＭＰモジュールが選択的に動作しているものとする。図示の例では、ＩＣカードとして提供されるＣＡＳモジュールはＲＭＰモジュール４６０の一部を構成する。

【０１４７】蓄積されたコンテンツを再生する際、該当する権利処理メタデータをハード・ディスク装置４５３から読み出す。

【０１４８】権利処理メタデータ中には、ＥＣＭ（Entitlement Control Message）とＥＭＭ（Entitlement Management Message）が含まれている。ＥＣＭは、ＣＡＳスクランブルを解除するためのスクランブル鍵Ｋｓｃを暗号化したものである。また、ＥＭＭは、ＥＣＭを解くためのワーク鍵を、契約期間などの契約内容やメッセージとともに暗号化したものである。

【０１４９】復号部４６２は、ＢＳ－ＣＡＳ ＩＣカードに記録されているマスター鍵Ｋｍを用いてＥＭＭを解読してワーク鍵と契約情報を得る。次いで、復号部４６１は、ワーク鍵を用いてＥＣＭを解読して、スクランブル鍵Ｋｓｃを得る。

【０１５０】判定部４６４は、復号部４６２において得られた契約情報に基づき、コンテンツ受信機４００Ｃの正当性を検証する。正当と判定した場合、スクランブル鍵Ｋｓｃを復号部４６５に供給する。

【０１５１】ハード・ディスク装置４５３に蓄積された受信コンテンツは、ＣＡＳに基づき、Ｍｕｌｔｉ２などの方式によりスクランブル処理されている。復号部４６５は、再生すなわち視聴したいコンテンツをハード・ディスク装置４５３から取り出して、スクランブル鍵Ｋｓｃを用いてデスクランブル処理する。

【０１５２】ＡＰＳ処理部４６６は、ビデオ信号などのアナログ出力信号に対して、マクロビジョンやＣＧＭＳ－Ａなどのコンテンツ保護処理を適用した後、再生コンテンツとしてテレビジョン（図示しない）などの出力装置に送出する。

【０１５３】一方、復号部４６２において得られた契約情報は、ＰＰＶデータ格納部４６３に蓄積される。ＲＭＰモジュール４６０は、定期的あるいは不定期的に管理センタ２０２に接続して、ＰＰＶデータを転送する。管理センタ２０２は、ＰＰＶデータを基に、コンテンツ利

用者に対する課金処理を行うことができる。

【0154】図12に示すコンテンツ受信機400Dの構成によれば、CASをそのまま蓄積コンテンツの課金に利用することができる。CASに従って暗号化されたコンテンツは、暗号化されたままハード・ディスク装置に蓄積される。CASで使用されるマスター鍵KmによりEMM並びにECMを解いて、蓄積コンテンツを解くことができる。その際、暗号を解いたことを課金ログとして記録する。このような課金ログを定期的あるいは不定期的に管理センタに送信することで、コンテンツ利用者に対して確実に課金を行うことができる。

【0155】また、図13には、放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例400Dの構成を模式的に示している。同図に示すコンテンツ受信機400Dは、ICカード化された衛星放送用のCASモジュール、すなわちBS-CAS ICカードを内蔵しており、CASシステムに基づいて衛星放送を限定受信してCASデスクランブルを行った後、再度暗号化してハード・ディスク装置に蓄積するタイプである。以下、同図を参照しながら、コンテンツ受信機400Dについて説明する。

【0156】受信コンテンツの権利処理はRMPモジュール480により行われる。RMPモジュール480は、ハードウェア・モジュールあるいはソフトウェア・モジュールいずれの形態で実装されていてもよい。フロント・エンド部（図示しない）よりコンテンツが受信されたときに、対応する権利処理メタデータが読み出され、RMP識別情報（RMP ID）が検出され、適当なRMPモジュールが選択的に動作しているものとする。同図に示す例では、ICカードとして提供されるCASモジュールや、ハード・ディスク装置に蓄積するコンテンツの保護を行うセキュア・モジュールは、RMPモジュール480の一部を構成する。セキュア・モジュールは、ハード・ディスク装置に蓄積するコンテンツの再暗号化処理、並びに、再生時の暗号解除処理を行う。

【0157】図示しないフロント・エンドにより受信されたデータ・コンテンツのうち、権利処理メタデータは、CASモジュールすなわちBS-CAS ICカードに入力される。

【0158】権利処理メタデータ中には、ECM（Entitlement Control Message）とEMM（Entitlement Management Message）が含まれている。復号部482は、BS-CAS ICカードに記録されているマスター鍵Kmを用いてEMMを解読してワーク鍵と契約情報を得る。次いで、復号部481は、ワーク鍵を用いてECMを解読して、スクランブル鍵Kscを得る。また、復号部482において得られた契約情報は、PPVデータ格納部483に蓄積される。

【0159】判定部484は、復号部482において得られた契約情報に基づき、コンテンツ受信機400Dの

正当性を検証する。正当と判定した場合、スクランブル鍵Kscを復号部485に供給する。

【0160】復号部485は、スクランブル鍵Kscを用いて受信コンテンツをデスクランブル処理して、セキュア・モジュールに出力する。

【0161】セキュア・モジュール内では、暗号化部487が、コンテンツ受信機400Dに固有のコンテンツ蓄積鍵Kstを用いてCASデスクランブル後のコンテンツを再度暗号化して、ハード・ディスク装置473に格納する。

【0162】また、ハード・ディスク装置473に蓄積しておいたコンテンツを再生すなわち視聴する場合には、暗号化コンテンツをハード・ディスク装置473から読み出し、復号部488にてコンテンツ蓄積鍵Kstを用いて復号化する。そして、APS処理部489は、ビデオ信号などのアナログ出力信号に対して、マクロビジョンやCGMS-Aなどのコンテンツ保護処理を適用した後、再生コンテンツとしてテレビジョン（図示しない）などの出力装置に送出する。

【0163】また、セキュア・モジュール内では、CASデスクランブル処理後のコンテンツから権利処理メタデータが取り出され、課金データとして蓄積される。

【0164】RMPモジュール480は、定期的あるいは不定期的に管理センタ202に接続して、CASモジュールにて蓄積されたPPVデータや、セキュア・モジュールにて蓄積された課金データを転送する。管理センタ202は、PPVデータを基に、コンテンツ利用者に対する課金処理を行うことができる。

【0165】図13に示すような構成のコンテンツ受信機400Dによれば、CASシステムに従って配信されるコンテンツを再度暗号化して、ハード・ディスク装置に蓄積することができる。再暗号化の際、CASで使用するスクランブル鍵Kscとは異なる鍵構造のコンテンツ蓄積鍵Kstで暗号化する。ハード・ディスク装置に蓄積された暗号化コンテンツを再生する場合には、再生する度に課金ログを生成して、定期的あるいは不定期的に管理センタ202に送信して、コンテンツ利用者に対する課金を行う。CASをRMPモジュールと一体化して構成することもできる。

【0166】【追補】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0167】

【発明の効果】以上詳記したように、本発明によれば、映画や音楽などの暗号化された形式で配信される有料コ

ンテンツを特定の利用者が好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【0168】また、本発明によれば、映画や音楽などのコンテンツ制作・提供業者が放送事業者やインターネット・サービス・プロバイダなどの仲介業者を介して配信する暗号化コンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【0169】また、本発明によれば、コンテンツ制作・提供業者自身がコンテンツ利用に関する課金やセキュリティなどを制御可能な形態で配信するコンテンツを好適に受信することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【0170】また、本発明によれば、各コンテンツ配信システム毎に策定される複数のRMP (Right Management & Protection) 方式に対応することができる、優れたコンテンツ受信装置及びコンテンツ受信方法を提供することができる。

【0171】本発明に係るコンテンツ受信装置及びコンテンツ受信方法によれば、1台のコンテンツ受信機を用いて複数の異なるコンテンツ配信方式に対応することができ、配信システム毎の受信機などの機器を用意する必要がなくなる。また、各コンテンツ制作・提供・配信事業者間では、RMP仕様記述などのコンテンツ配信方式の規格化をめぐる争いを沈静化することができる。また、各コンテンツ制作・提供・配信事業者間における配信コンテンツの互換性や融通性を向上させることができる。また、コンテンツ利用者においては、利便性が高まる。

【図面の簡単な説明】

【図1】RMPモジュールの概念構成を示した図である。

【図2】異なるRMP仕様を実装した複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用する形式のコンテンツ受信機の構成を模式的に示した図である。

【図3】異なるRMP仕様を実装した複数のハードウェアRMPモジュールを用意しておき、各受信コンテンツ毎に適合するハードウェアRMPモジュールに切り替えて利用する形式のコンテンツ受信機20の他の構成例を模式的に示した図である。

【図4】ソフトウェア・モジュールとしてRMPモジュールを構成し、各受信コンテンツ毎に適合するソフトウェア・モジュールを所定のサーバからダウンロードする形式のコンテンツ受信機30の他の構成例を模式的に示した図である。

【図5】コンテンツ受信機30にRMPモジュールをダウンロードするための処理手順を示したフローチャートである。

【図6】ソフトウェアRMPモジュールをコンテンツ受信機30内部で自動生成するための処理手順を示したフローチャートである。

【図7】コンテンツ配信システムの概略的構成を示した図である。

【図8】コンテンツ制作並びに配信を行う放送局における構成を模式的に示した図である。

【図9】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の一例400Aの構成を模式的に示した図である。

【図10】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例400Bの構成を模式的に示した図である。

【図11】図9に示したコンテンツ受信機400Aにおいて、受信コンテンツをハード・ディスク装置413Aに蓄積するための処理手順の一例を示したフローチャートである。

【図12】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例400Cの構成を模式的に示した図である。

【図13】放送波として搬送される配信コンテンツを受信するコンテンツ受信機の他の例400Cの構成を模式的に示した図である。

【図14】CASベースのコンテンツ配信システムの概観構成を示した図である。

【符号の説明】

10…コンテンツ受信機、11…フロント・エンド部
12…CAS処理部、13A，13B…ハード・ディスク装置
14…RMP識別部
20…コンテンツ受信機、21…フロント・エンド部
23…ハード・ディスク装置、24…RMP識別部
25…デコーダ出力装置
30…コンテンツ受信機、31…フロント・エンド部
32…CPU、33A，33B…ハード・ディスク装置
34…RMP識別部、35…作業メモリ
36…デコーダ出力装置、37…ネットワーク・インターフェース
200…コンテンツ・プロバイダ
201…番組制作会社（委託放送事業者）、202…管理センタ（決済機関）
250…認証局
300…放送局（衛星放送受託放送事業者）、301…放送衛星
311…コンテンツ暗号化部、312…コンテンツ鍵暗号化部
313…マルチプレクサ、314…CASスクランブラ
400…コンテンツ受信機（コンテンツ配信対応衛星放送受信機）

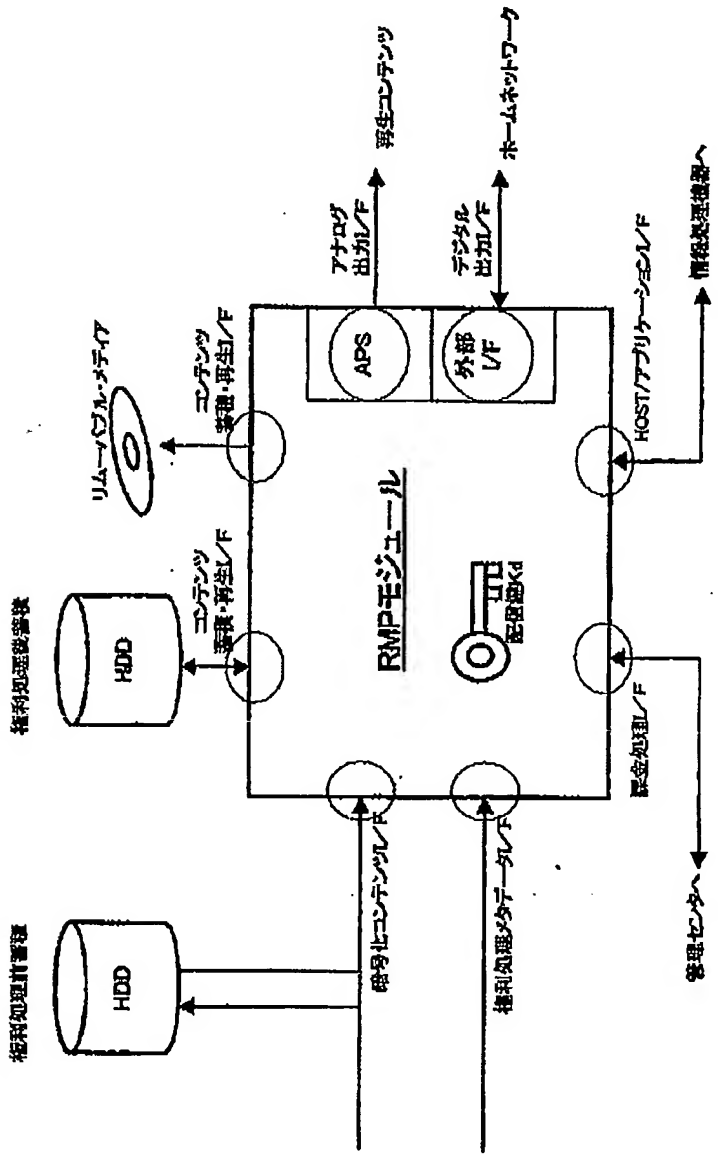
33

411…CASデスクランブラ、412…デマルチプレクサ
413A，413B…ハード・ディスク装置
420…RMPモジュール、421…コンテンツ鍵復号化部
422…コンテンツ鍵再暗号化部
433…ハード・ディスク装置、440…RMPモジュール
441…コンテンツ鍵復号化部、442…コンテンツ復号化部
443…APS処理部

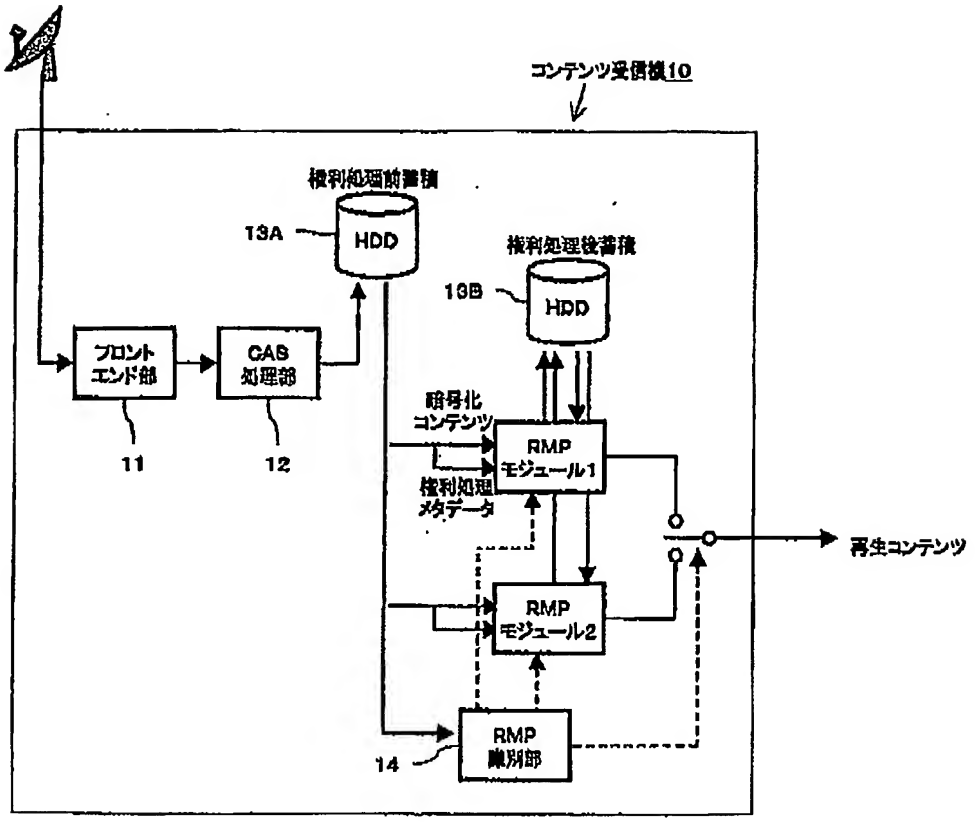
34

＊453…ハード・ディスク装置、460…RMPモジュール
461…復号部、462…復号部
463…PPVデータ格納部、464…判定部
465…復号部、466…APS処理部
473…ハード・ディスク装置、480…RMPモジュール
481…復号部、482…復号部
483…PPVデータ格納部、484…判定部
485…復号部、487…暗号化部
488…復号部、489APS処理部

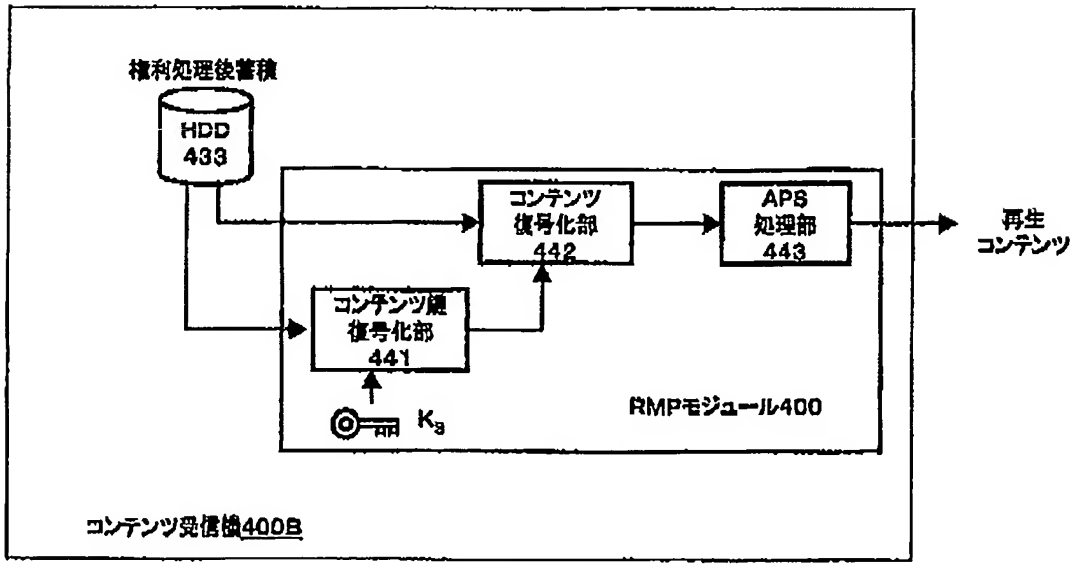
【図1】



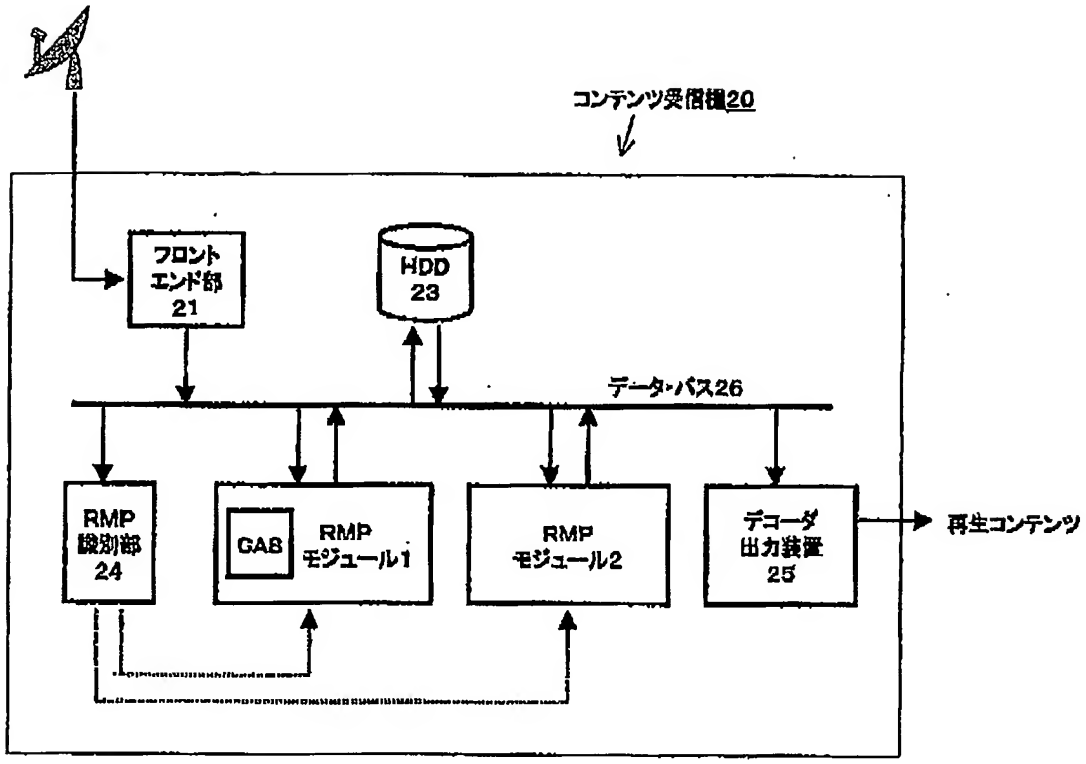
【図2】


コンテンツ受信機10
権利処理前蓄積
13A
HDD
権利処理後蓄積
13B
HDD
フロントエンド部
CAS処理部
11
12
暗号化コンテンツ
権利処理メタデータ
RMPモジュール1
RMPモジュール2
RMP識別部
14
再生コンテンツ

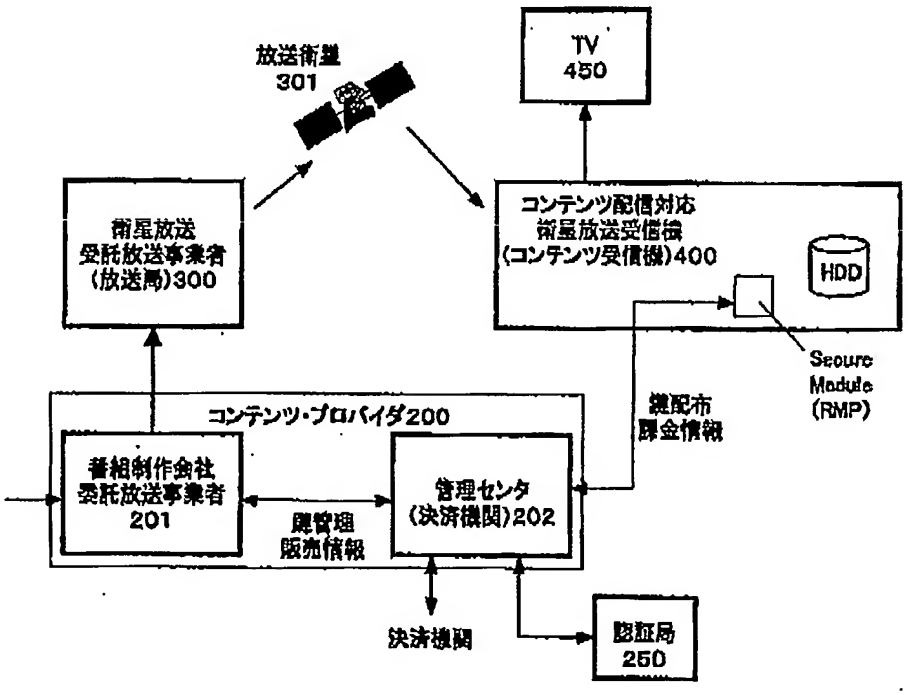
【図10】


権利処理後蓄積
HDD
433
コンテンツ復号化部
442
APS処理部
443
再生コンテンツ
コンテンツ鍵復号化部
441
K_s
RMPモジュール400
コンテンツ受信機400B

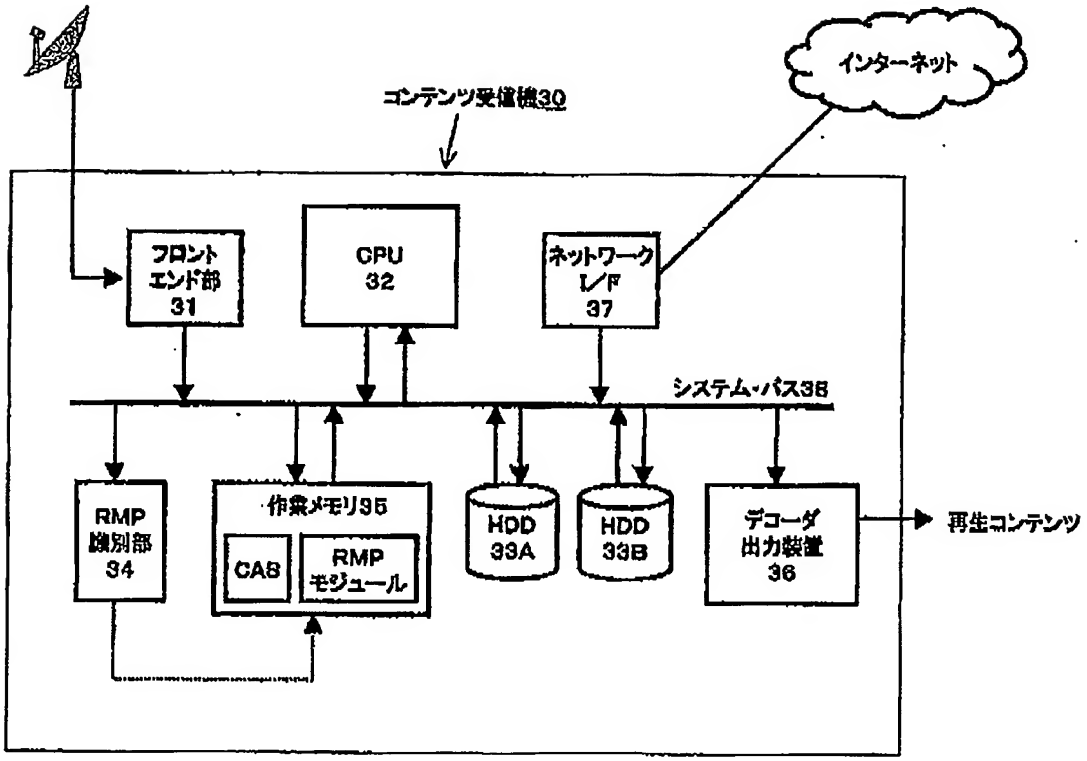
【図3】


コンテンツ受信機20
フロントエンド部21
HDD23
データ・バス26
RMP識別部24
GAB
RMPモジュール1
RMPモジュール2
デコーダ出力装置25
再生コンテンツ

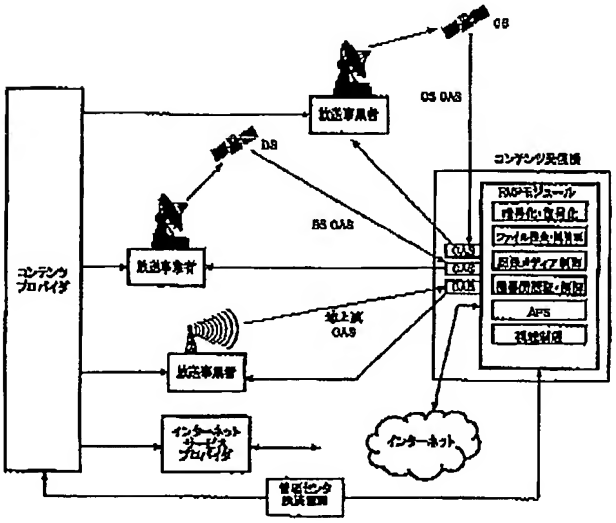
【図7】


放送衛星301
TV450
衛星放送受託放送事業者(放送局)300
コンテンツ配信対応衛星放送受信機(コンテンツ受信機)400
HDD
Secure Module (RMP)
コンテンツ・プロバイダ200
課金情報
番組制作会社委託放送事業者201
課管理販売情報
管理センタ(決済機関)202
決済機関
認証局250

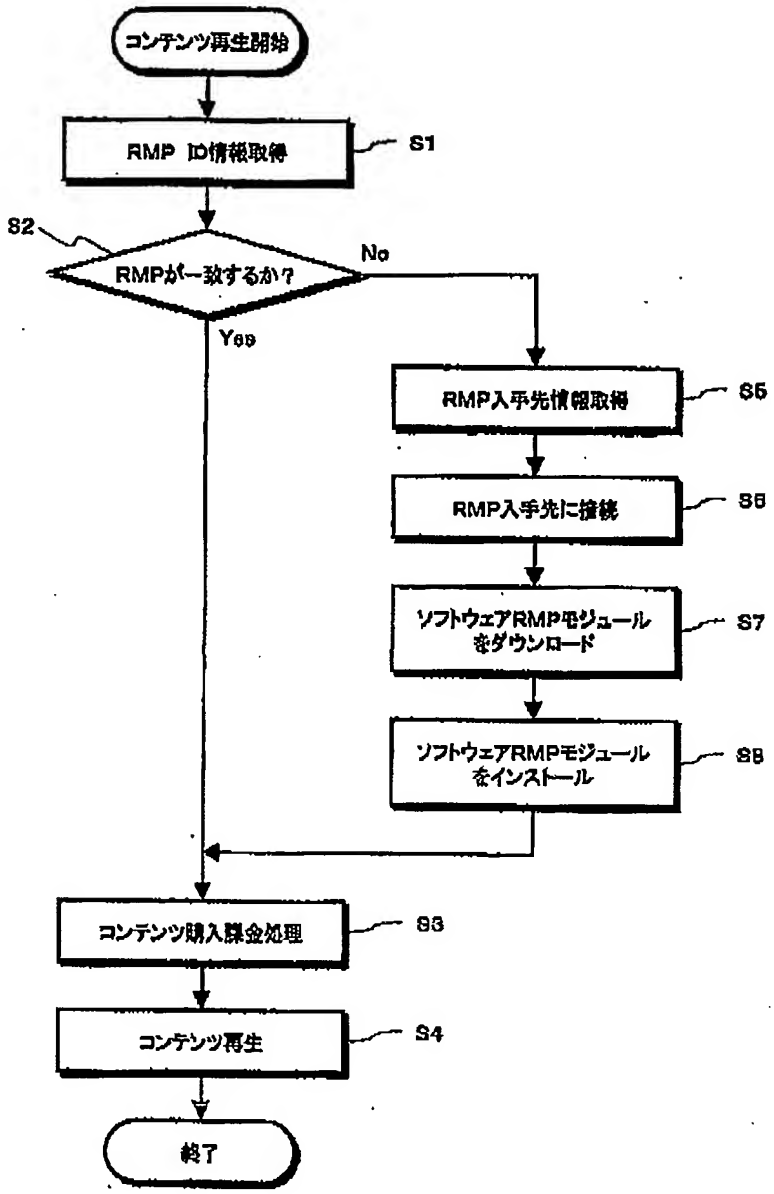
【図4】


インターネット
コンテンツ受信機30
フロント
エンド部
31
CPU
32
ネットワーク
I/F
37
システム・バス38
RMP
識別部
34
作業メモリ35
CAS
RMP
モジュール
HDD
33A
HDD
33B
デコーダ
出力装置
36
再生コンテンツ

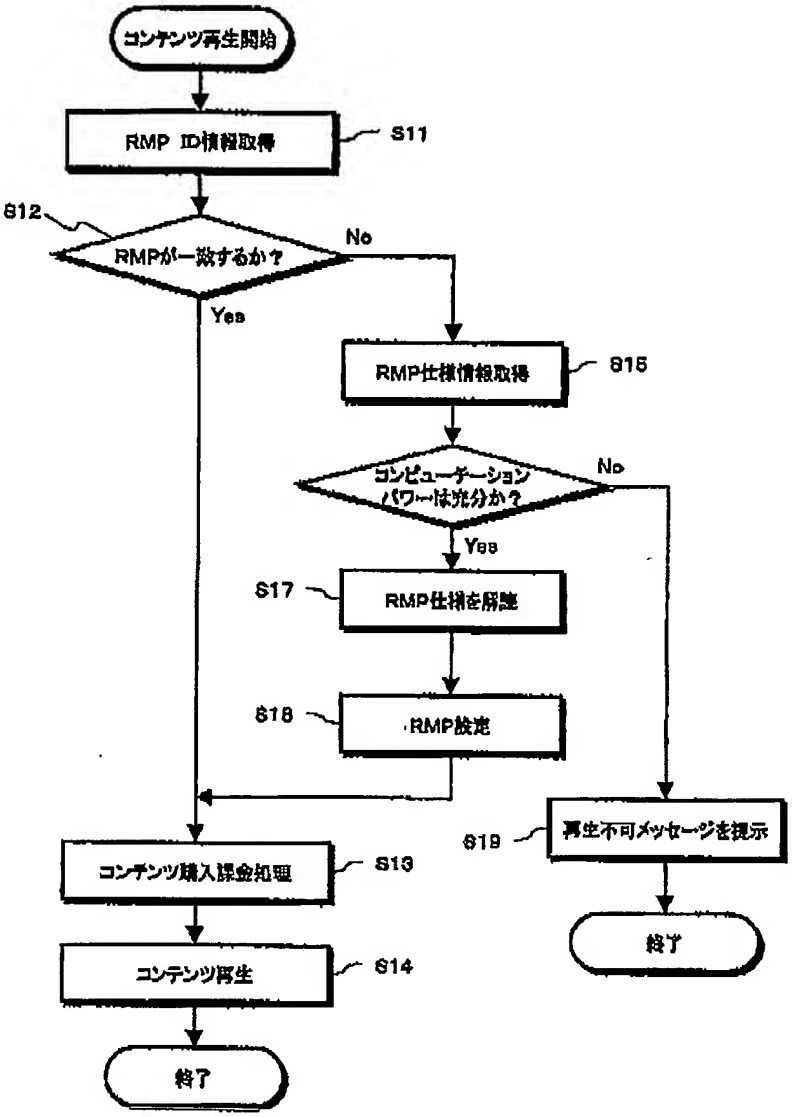
【図14】


CS
CS CAS
放送事業者
BS
BS CAS
コンテンツ受信機
RMPモジュール
CAS
APS
コンテンツ
プロバイダ
放送事業者
地上波
CAS
放送事業者
インターネット
サービス
プロバイダ
インターネット

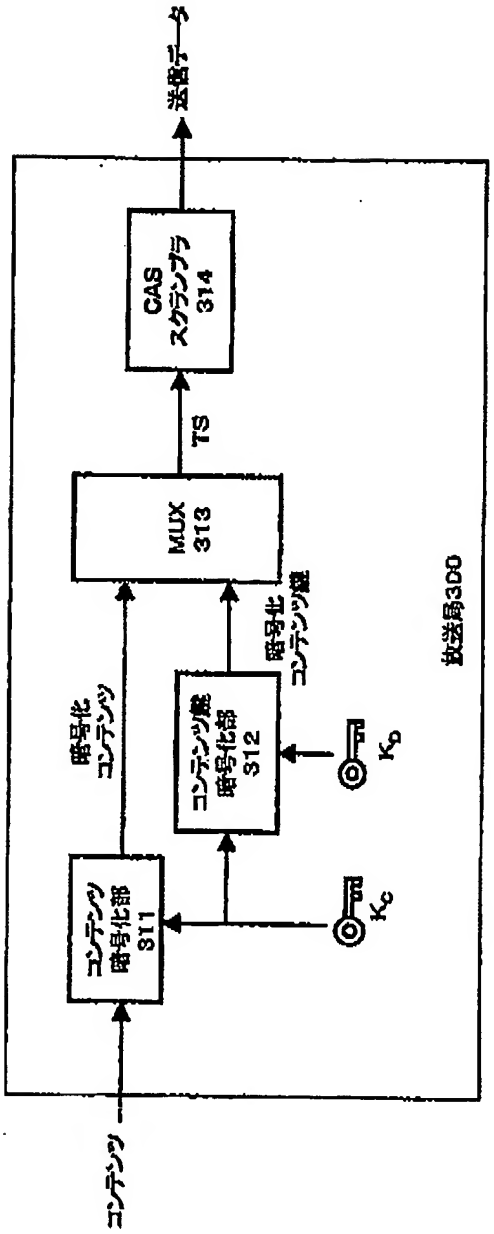
【図5】


コンテンツ再生開始
RMP ID情報取得
S1
S2
RMPが一致するか?
No
Yes
RMP入手先情報取得
S5
RMP入手先に接続
S6
ソフトウェアRMPモジュールをダウンロード
S7
ソフトウェアRMPモジュールをインストール
S8
コンテンツ購入課金処理
S3
コンテンツ再生
S4
終了

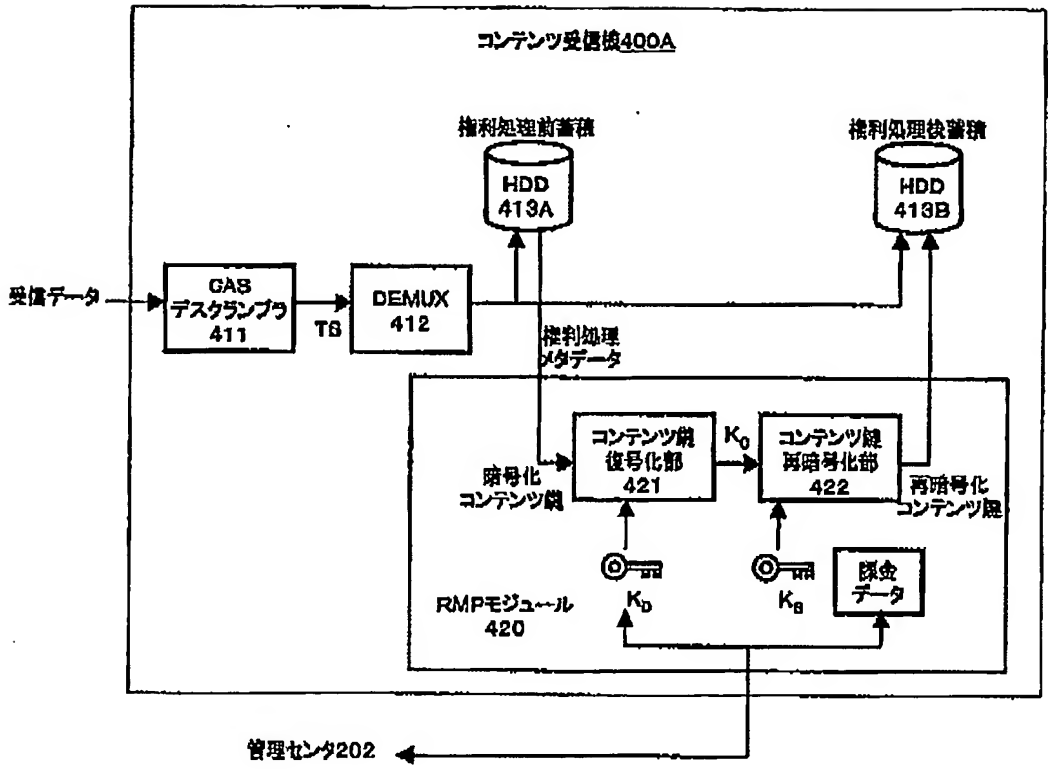
【図6】


コンテンツ再生開始
RMP ID情報取得
S11
S12
RMPが一致するか？
No
Yes
RMP仕様情報取得
S15
コンピューテーション
パワーは充分か？
No
Yes
S17
RMP仕様を解読
S18
RMP設定
S19
再生不可メッセージを提示
終了
コンテンツ購入課金処理
S13
コンテンツ再生
S14
終了

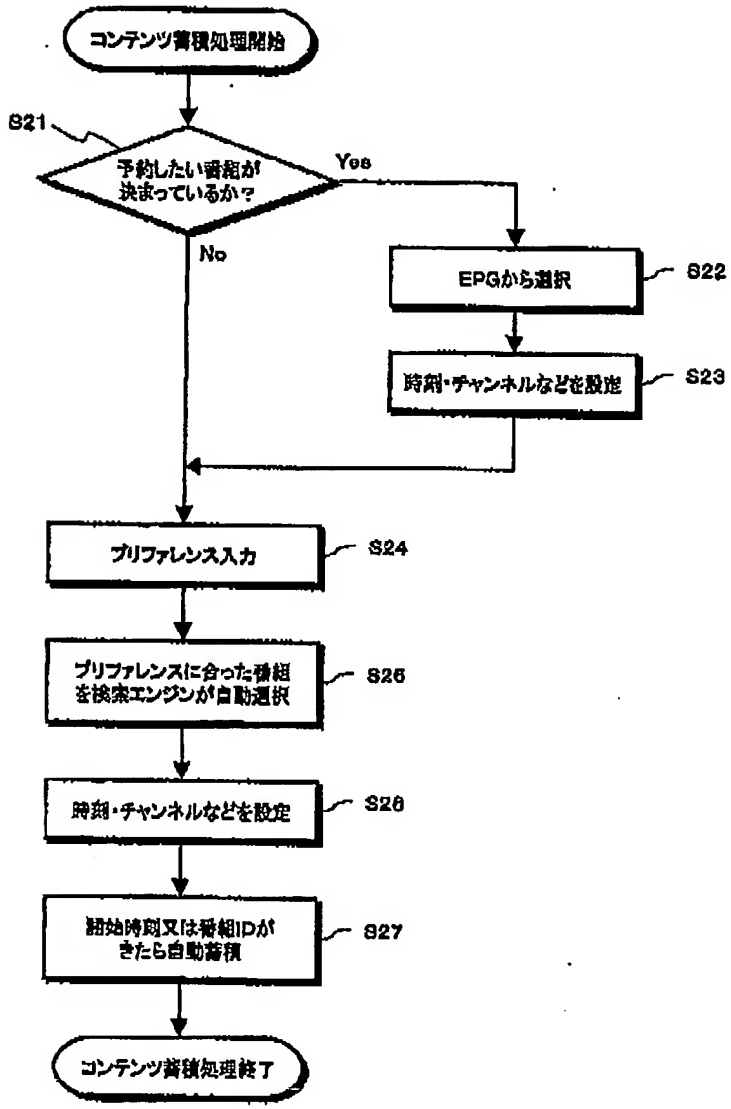
【図8】


送信データ
CAS スクランブラ 314
TS
MUX 313
暗号化コンテンツ鍵
暗号化コンテンツ
コンテンツ鍵暗号化部 312
コンテンツ暗号化部 311
K_D
K_C
放送局300
コンテンツ

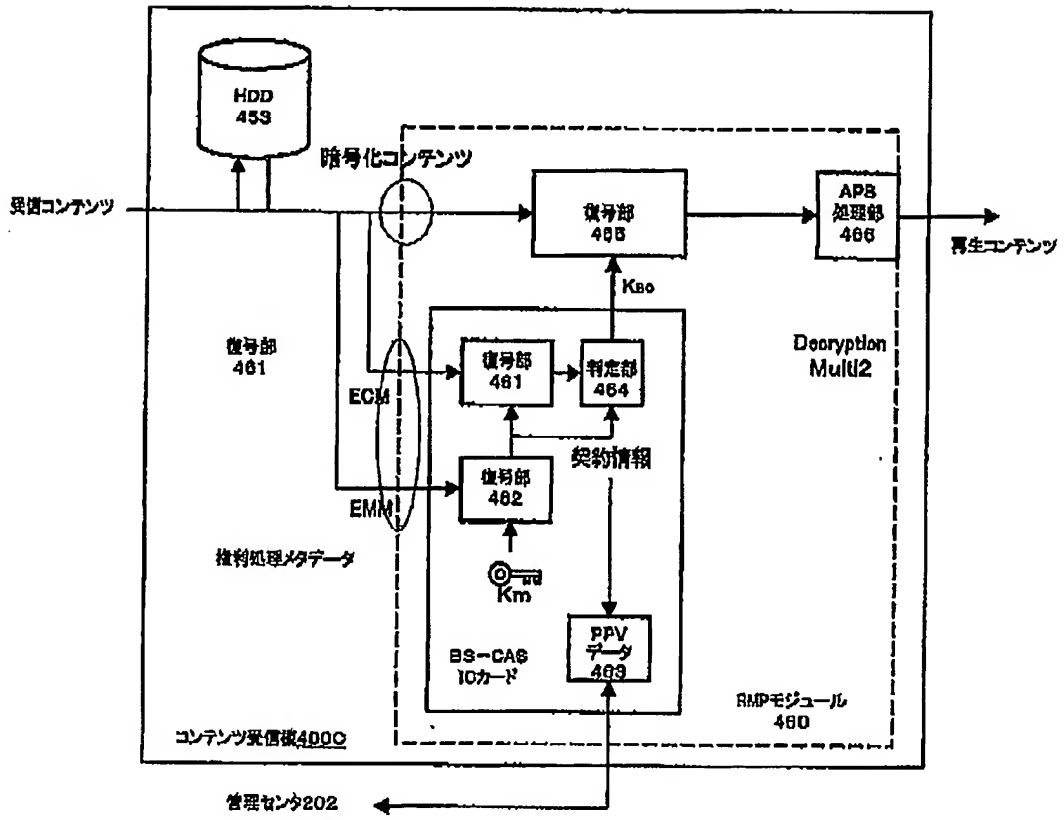
【図9】


コンテンツ受信機400A
権利処理前蓄積
HDD
413A
権利処理後蓄積
HDD
413B
受信データ
GAS
デスクランブラ
411
TS
DEMUX
412
権利処理
メタデータ
暗号化
コンテンツ鍵
コンテンツ鍵
復号化部
421
K_D
コンテンツ鍵
再暗号化部
422
再暗号化
コンテンツ鍵
RMPモジュール
420
K_D
K_B
課金
データ
管理センタ202

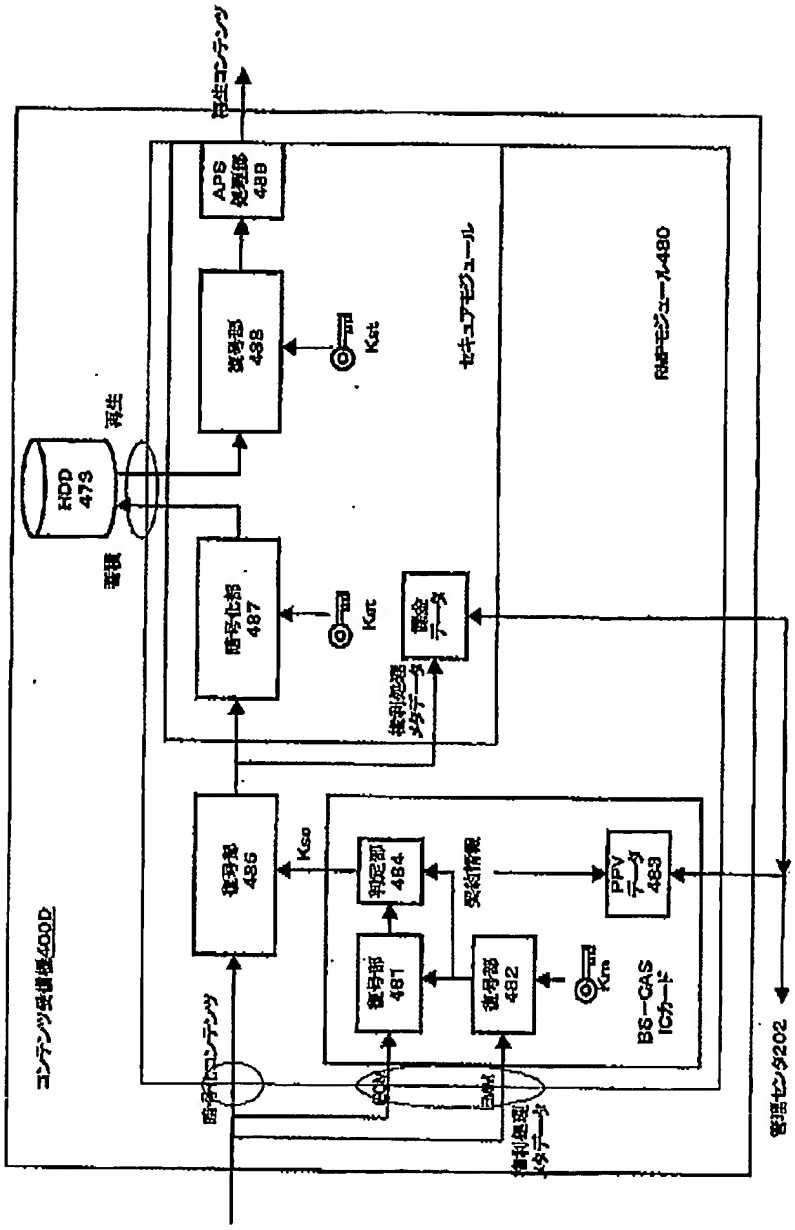
【図11】


コンテンツ蓄積処理開始
S21
予約したい番組が決まっているか？
Yes
No
EPGから選択
S22
時刻・チャンネルなどを設定
S23
プリファレンス入力
S24
プリファレンスに合った番組を検索エンジンが自動選択
S25
時刻・チャンネルなどを設定
S26
開始時刻又は番組IDがきたら自動蓄積
S27
コンテンツ蓄積処理終了

【図12】


HDD
453
暗号化コンテンツ
受信コンテンツ
復号部
455
APS
処理部
466
再生コンテンツ
Kso
復号部
461
Decryption
Multi2
ECM
復号部
461
判定部
464
契約情報
EMM
復号部
462
権利処理メタデータ
Km
PPV
データ
463
BS−CAS
ICカード
RMPモジュール
460
コンテンツ受信機4000
管理センタ202

【図13】



フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード(参考)
H04N 7/167		H04L 9/00	601E	
		H04N 7/167	Z	

Fターム(参考) 5B085 AA08 AE00 AE29
5C025 BA25 BA27 DA04 DA05
5C064 BA01 BB01 BC03 BC06 BC22
BC25 BD04 BD09 BD14 CA14
5J104 AA01 AA12 AA15 AA16 EA06
EA18 NA02 NA35 NA37 PA05
PA07 PA11